FEDERAL HIGHWAY ADMINISTRATION

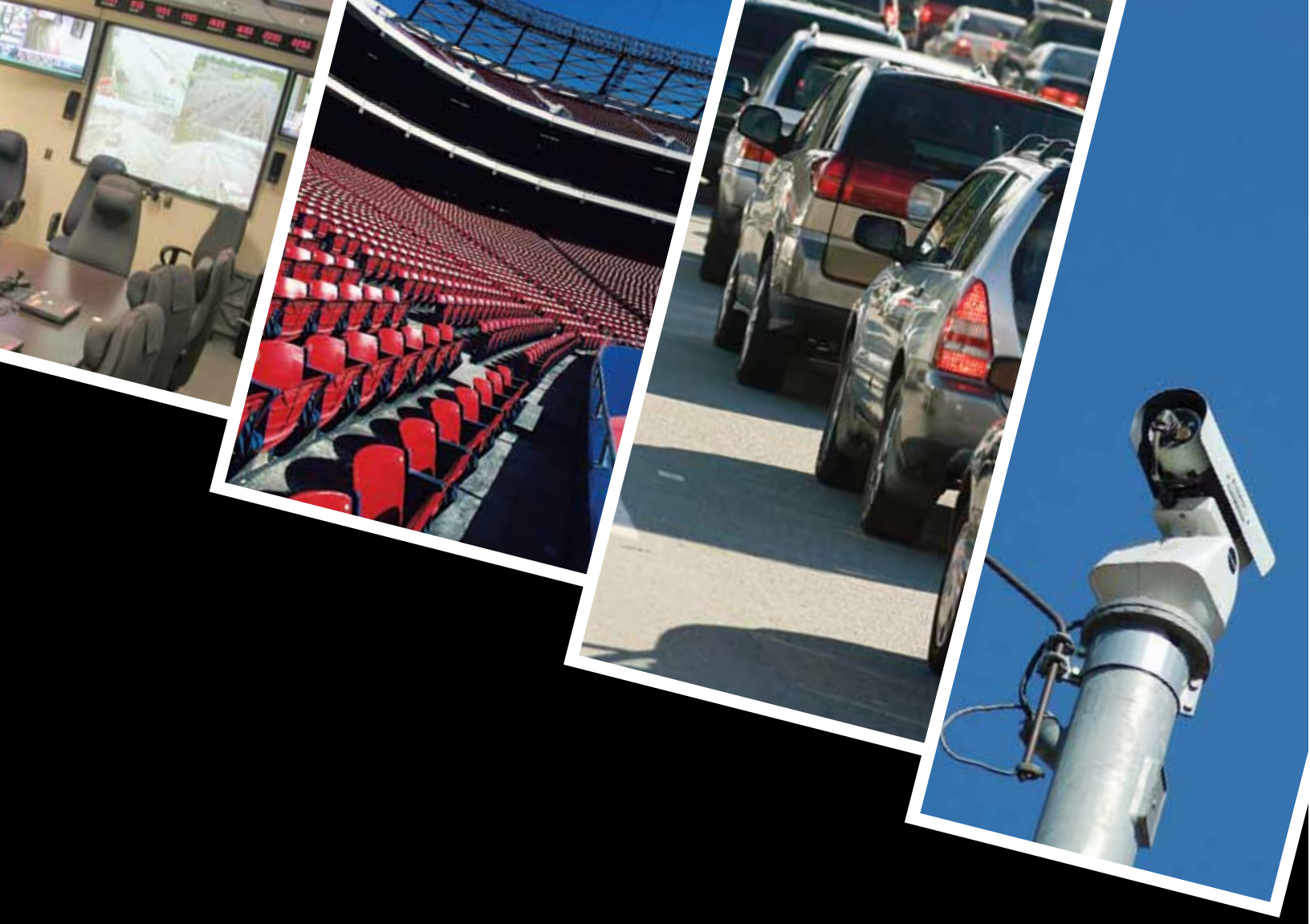
INFORMATION-SHARING GUIDEBOOK

FOR

TRANSPORTATION MANAGEMENT CENTERS, EMERGENCY OPERATIONS CENTERS, AND FUSION CENTERS

June 2010

U.S. Department of Transportation
Federal Highway Administration



NOTICE

This document is disseminated under the sponsorship of the department of transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof. This report does not constitute a standard, specification, or regulation.

The United States Government does not endorse products or manufacturers. Trade and manufacturers' names appear in this report only because they are considered essential to the object of the document.

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-HOP-09-003		

4. Title and Subtitle	5. Report Date
Information Sharing Guidebook for Transportation Management Centers, Emergency Operations Centers, and Fusion Centers	June 2010
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
Nancy Houston, John Wiegmann, Robin Marshall, Ram Kandarpa, John Korsak, Craig Baldwin, Jeff Sangillo, Susan Knisely, Kevin Graham, Andrea Vann Easton	

9. Performing Organization Name and Address		10. Work Unit No. (TRAIS)
Booz Allen Hamilton 8283 Greensboro Drive McLean, Virginia 22102	HNTB Corporation 11414 West Park Place, Suite 300 Milwaukee, WI 53224	11. Contract or Grant No.

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
Federal Highway Administration, HOTO-1 U. S. Department of Transportation 1200 New Jersey Avenue SE Washington, D. C. 20590	Final Report
	14. Sponsoring Agency Code HOTO, FHWA

15. Supplementary Notes

Kimberly Vasconez, FHWA Team Leader, Emergency Transportation Operations, Contracting Officer's Technical Representative (COTR)

16. Abstract

This guidebook provides an overview of the mission and functions of transportation management centers, emergency operations centers, and fusion centers. The guidebook focuses on the types of information these centers produce and manage and how the sharing of such information among the centers can be beneficial to both the day-to-day and emergency operations of all the centers. Challenges exist to the ability to share information, and the guidebook addresses these challenges and options for handling them. The guidebook also provides some lessons learned and best practices identified from a literature search and interviews/site visits with center operators.

17. Key Words	18. Distribution Statement
Transportation Management Center, Traffic Management Center, Transportation Operations Center, Emergency Operations Center, Fusion Center	No restrictions.

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified.	Unclassified.	144	

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1. INTRODUCTION

Transportation management centers (TMCs) exist in many large population and traffic concentration areas across the country to manage and enhance the efficient operation, safety, and health of major metropolitan and regional transportation networks and corridors. TMCs perform a wide variety of transportation management functions, depending on the authority and capability vested in the centers. Table 1-1 lists the most common TMC functional areas.

Table 1-1: TMC Common Functional Areas

TMC Common Functional Areas
Management of traffic control systems and assets
Incident response and clearance functions
Emergency response functions
Monitoring and surveillance of transportation network conditions
Acquisition and communication of traffic information

The extent of the leading and supporting roles of TMCs in these functional areas varies depending on specific jurisdictional situations, incidents, or emergencies. TMCs are also sometimes referred to as traffic management centers or transportation or traffic operations centers (TOCs). While there is no standard definition for these terms, those referred to as *transportation* rather than *traffic* may have a multi-modal focus—not just a roadway focus. Those centers referred to as *operations* rather than *management* centers may have a larger role in overall transportation operations, including incident management, through a more fully integrated team with law enforcement and other emergency responders as well as other proactive response functions such as operating a safety/service patrol.

Emergency operations centers (EOCs) exist in some form in virtually every State and local jurisdiction in the country. Their primary roles include management of and response to emergencies of all kinds that threaten or result in significant impact on public health and safety, infrastructure, commerce, and/or national security. EOCs typically are communications centers and physical locations where responsible government officials, along with law enforcement, fire, emergency medical services (EMS), and infrastructure management authorities, gather to coordinate emergency response. EOCs usually define and tier coordination and leadership roles along jurisdictional lines, and full operations of these centers are "stood up" according to defined criteria for declaring emergency conditions.[1] Table 1-2 lists the most common EOC functional areas.

1 Many EOCs continuously staff personnel to maintain preparedness and monitor alerts and developing conditions that may lead to declared emergencies. In emergencies, designated officials assemble and manage operational decisions from or through the center.

Table 1-2: EOC Common Functional Areas

EOC Common Functional Areas
Communications management and coordination
Physical facility for assembly of responsible officials and staff
Emergency response decision-making and management of response functions
Monitoring and surveillance of emergency situation and response activity

According to the *Fusion Center Guidelines*, a fusion center (FC) is a collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity. Some forms of FCs address specific laws such as driver licensing, banking crime, or specific critical infrastructure elements. At the same time, some FCs also exist to synthesize information and focus on a much wider set of public safety and national security challenges (such as terrorism, major criminal activities, public health risks, major economic risks, critical infrastructure protection, and major natural hazards). Table 1-3 lists the most common FC functional areas.

Table 1-3: FC Common Functional Areas

FC Common Functional Areas
Aggregation and synthesis of safety and security-related information
Assessment and reporting of safety and security threats
Monitoring and surveillance of critical infrastructure conditions

The three types of centers distinctly differ in their primary missions, and each center type acquires and processes information that is unique and may not be of common interest. **However, significant actual and potential information exchange can benefit the centers' assessments, decision-making, and operations.**

The potential benefits of TMC, EOC, and FC center-to-center information sharing are most apparent when addressing the centers' common uses of various types of information about regional and local transportation networks. Categories of transportation information best suited for common use or exchange are those regarding configuration, operations status, and incidents on the transportation network. This guidebook addresses sharing[2] of transportation information between centers and explores information-sharing logic, benefits, barriers, and solutions.

2 Many EOCs continuously staff personnel to maintain preparedness and monitor alerts and developing conditions that may lead to declared emergencies. In emergencies, designated officials assemble and manage operational decisions from or through the center.

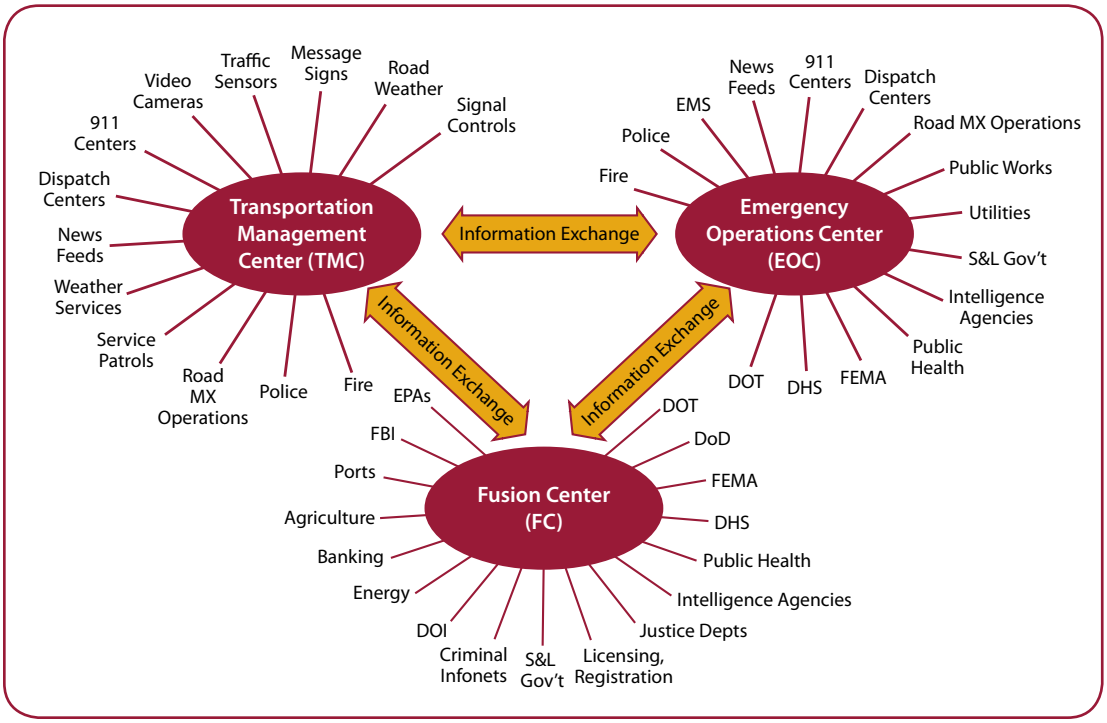
1.1 The Information-Sharing Situation Today

TMCs, EOCs, and FCs have established information-gathering and communications channels that tap into external sources, as well as "owned" equipment and operations systems. They interconnect with partner agencies and with deployed assets (e.g., cameras, sensors, and control systems) via landline, wireless, and Internet links. Key external communications links for TMCs and EOCs also include weather services, 911 centers, law enforcement dispatch systems (e.g., computer-aided dispatch [CAD] and similar systems), and the traffic reporting media.

Communications links for the many variations of FCs are more difficult to characterize because they are very specific to the particular criminal, safety, or hazard focus of each center. FCs employ landline, wireless, and Internet links, and, where practical, integrated data systems. Often, the data and communication connections include law-enforcement-sensitive or classified information, so equipment for relaying information is specialized.

Figure 1-1 characterizes the centers' respective information sources, using linkages that are representative of the various centers researched.

Figure 1-1: Centers' Links



Each EOC maintains seats and terminals dedicated for any local or regional agency that might be engaged in particular emergencies (e.g., police, fire, public works, transit, and intelligence agencies; EMS; TMCs; departments of transportation; and bridge, tunnel, and toll road authorities) and represents a functional area (e.g., transportation and mass care). Principal agencies involved in the specific FC missions jointly staff the FCs.

The trend in and importance of information sharing is on the rise today, as more resources have been invested in sophisticated intelligent transportation systems (ITS) and surveillance technologies, as major terrorist and natural emergencies have overstressed real-time communications, and as increasingly congested roadways lead to incidents that impede traffic flows and threaten lives and property. These incidents have clearly shown the high public costs of information gaps, preparedness deficiencies, and insufficient situational awareness by decision-makers.

While many kinds of information sharing can be logical and useful for TMC, EOC, and FC missions, achieving the sharing of information can require significant dedication and investment in the proposition. Legitimate and significant technical and policy barriers to information exchange can come into play and must be resolved. This guidebook explores the following hurdles:

- Legal and privacy concerns related to surveillance and traveler information
- Control and security of criminal and potentially litigious information
- Prudent and appropriate release of information to the public domain
- Varying levels of concern between centers over security, reliability, and sustainability of specific information flows
- "Language" complexities, including data and message standards, geo-referencing systems, usage conventions
- Technical barriers in linking together legacy media, hardware, and systems (e.g., digital video feeds and multiple wireless standards and frequencies)
- Specific policies and mandates of participating agencies—regarding ownership of resources, mission priorities, and logical and physical access restrictions.

The communication and information-sharing barriers are classic problems—both complicated and frequently addressed by policy-makers and practitioners with irony and resignation. As the challenges that TMCs, EOCs, and FCs face continue to grow more complex, policy practices are becoming more sophisticated and improved technologies are facilitating better ways to gather, process, properly synthesize, and share information.

1.2 The Potential Value of Sharing Transportation-Related Information

TMCs, EOCs, and FCs similarly gather, process, and synthesize at least three basic kinds of information to make operational decisions or reach conclusions on actions needed:

- **Operational Information (Situational)** – Critical for making fast and informed operational decisions and for communicating accurate alerts and notifications on incidents, threats, and emergencies
- **Recorded Information** – Basis for operational assessments, investigation, planning, and after-action reporting

- **Physical Infrastructure Information** – Framework for setting and communicating priorities, determining risks, and deploying field resources.

Table 1-4 presents these common information types and potential value to centers, characterized by transportation network examples.

Table 1-4: Common Information Types Across Centers

Information Type	Transportation Information Examples	Application		
		TMC	EOC	FC
Operational	Traffic flows, video feeds, localized surface weather	Traffic control, snow/ice tactics	Assessment of emergency situation and risks	Real-time threat, risk assessment
Recorded	Incident logs, video records, traffic records	Traffic safety assessment and planning	After-action assessment	Law enforcement, investigation
Physical Infrastructure	Maps, physical feature data	Work zone management, resource deployment	Data and framework for decisions, communications	Framework for threat, risk assessment

Information handled by EOCs can assist and enhance fulfillment of TMC and FC missions. Most of the information handled by EOCs during incident operations falls in the real-time category—in the form of alerts and notifications and advance indications of needs for transportation support from the transportation representatives at the EOC. Those transportation representatives at the EOC will need to maintain contact with their TMC, if not co-located, to ensure they keep the EOC up to date on traffic conditions and other such real-time situational information that can be supplied by the TMCs. Information coordinated by EOCs during and after emergency operations may also assist some FCs in their investigative and threat assessment roles.

Advanced FC information on threat assessment and critical infrastructure vulnerabilities would also assist TMCs and EOCs in planning and managing emergency preparedness, response, and recovery operations as well as inform potential future investments in transportation infrastructure.

Over the next 10 years, traffic and congestion challenges will continue to build rapidly in urban areas. Transportation managers will likely deploy more advanced traffic management and tolling technologies, and will no doubt integrate more multi-modal operations data to provide a more robust picture of the total transportation network in a region. Vehicle Infrastructure Integration (VII) or IntelliDrive℠ initiatives will ultimately lead to more proactive control[3] systems for transportation movements during emergencies. This evolution will likely enable TMCs to share more comprehensive "situational awareness" information to

3 Enabled by navigation systems, roadside dedicated short-range communications (DSRC), vehicle location, and speed data.

enhance EOC and FC operations. More fully integrated EOC voice and data communications systems will enable these centers to better and more quickly leverage outside information sources.

1.3 Guidebook Content

The purpose of this guidebook is to explore the possibilities, challenges, and logical benefits for increased information sharing between TMCs, EOCs, and FCs. The intent is to interest center managers and operators in new collaborative initiatives that may not have been considered and to provide information that may assist interested practitioners and policymakers in pursuing those new initiatives.

The remainder of the guidebook includes the following chapters:

- Chapter 2. Missions and Characteristics – Describes the TMC, EOC, and FC characteristics, functions, and information handled
- Chapter 3. Opportunities for Collaboration – Describes the information exchange opportunities
- Chapter 4. Challenges and Options for Information Exchange – Describes the technical and policy challenges
- Chapter 5. Lessons Learned and Successful Practices – Provides lessons learned in practice
- Chapter 6. Summary – Assessing the Value of TMC/EOC/FC Information-Sharing.

California Emergency Management Agency Preparedness Division

California State Emergency Operations Center

CHAPTER 2. MISSIONS AND CHARACTERISTICS

This chapter provides the current footprint, mission statement, and operational perspectives for TMCs, EOCs, and FCs. It also defines the following for each type of center:

- Roles and characteristics
- Statistics, locations, and jurisdictions
- Processes and operations
- System capabilities and resources
- Information managed and exchanged
- Communications links.

2.1 Roles and Characteristics

The roles and characteristics of TMCs, EOCs, and FCs are distinctive yet related in many areas of responsibilities and incident management. Table 2-1 provides descriptions of TMCs, EOCs, and FCs, as defined by various relevant institutions.

Table 2-1: Operations Management Center Descriptions

Type of Center	Description
Transportation Management Center	The Institute of Transportation Studies at the University of California-Berkley summarized the mission of a TMC as "the hub of a transportation management system, where information about the transportation network is collected and combined with other operational and control data to manage the transportation network and to produce traveler information. It is the focal point for communicating transportation-related information to the media and the motoring public, a place where agencies can coordinate their responses to transportation situations and conditions. The TMC links various elements of Intelligent Transportation Systems such as variable message signs, closed circuit video equipment, roadside count stations, etc., enabling decision makers to identify and react to an incident in a timely manner based on real-time data."

Type of Center	Description
Emergency Operations Center	The National Incident Management System[4] defines EOCs as "The physical location at which the coordination of information and resources to support domestic incident management activities normally takes place. An EOC may be a temporary facility or may be located in a more central or permanently established facility, perhaps at a higher level of organization within a jurisdiction. EOCs may be organized by major functional disciplines (e.g., fire, law enforcement, and medical services), by jurisdiction (e.g., Federal, State, regional, county, city, tribal), or some combination thereof."[5]
Fusion Center	The *Fusion Center Guidelines* developed by the U.S. Department of Justice and U.S. Department of Homeland Security define an FC as "a collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity."[6] The core function of a fusion center is the intelligence process. Simply stated, the "intelligence process" (or cycle) is an organized process by which information is gathered, assessed, and distributed.

2.1.1 TMC Overview

TMCs are responsible for a variety of functions to improve traffic conditions on transportation infrastructure, including highways, arterials, and transit, to increase efficiency and safety. In addition to personnel, ITS technologies located at the TMC and embedded in the infrastructure support TMC functions, some serving to support multiple functions. ITS represents an additional area of core functionality of TMC operations. To make these improvements in line with long-term strategic planning, regional TMCs implement ITS, which are used to monitor and control traffic. However, each region faces different transportation issues, including variations in geography, congestion issues, and incidents. Current planning for TMCs envisions their use as dispatch centers for local, regional, and State transportation assets, such as safety/service patrols and road maintenance efforts, leading to a more operational role. Some TMCs and TOCs already function in these capacities.

2.1.2 EOC Overview

EOCs coordinate information and resources to support domestic incident management activities. EOCs generally participate in both preparing for and responding to such incidents. For example, an EOC may support the evacuation of a community threatened by an incident such as a hazardous materials release or wildfire threat; response operations during a hurricane, tornado, or earthquake; and recovery activities following a flood, terrorist, or other malicious incident.

4 On February 28, 2003, the President issued Homeland Security Presidential Directive (HSPD)–5, Management of Domestic Incidents, which directs the Secretary of Homeland Security to develop and administer a National Incident Management System (NIMS). This system provides a consistent nationwide template to enable Federal, State, local, and tribal governments and private-sector and nongovernmental organizations to work together effectively and efficiently to prepare for, prevent, respond to, and recover from domestic incidents, regardless of cause, size, or complexity, including acts of catastrophic terrorism.

5 U.S. Department of Homeland Security, *National Incident Management System*, March 1, 2004. Page 129.

6 U.S. Department of Homeland Security and U.S. Department of Justice, *Fusion Center Guidelines*.

As noted in Section 2.1, the National Incident Management System (NIMS) definition recognizes that implementation of these centers may occur in a variety of ways based on several parameters, including:

- **Persistence** – Some operate on a continuous basis. Others are activated only in response to an incident; once the incident has been resolved, they are de-activated.
- **Functional Discipline** – In some implementations, an EOC may address a single functional discipline (e.g., law enforcement or medical services). In others, an EOC may address any combination of functional disciplines.
- **Jurisdiction** – EOCs may function at the Federal, State, regional, county, city, or tribal jurisdictional levels.

A combination of the persistence, functional, and jurisdictional parameters provides the basis for the implementation of a particular EOC. As with an EOC's operating status (e.g., incident-driven or standing) or organization, the resources available to an EOC directly reflect the community's particular needs and investment in emergency operations. Regardless of how an EOC is implemented, a functional transportation infrastructure (and current information on the condition of that infrastructure) is critical to the EOC's ability to accomplish its mission of facilitating the community's preparation for, response to, and recovery from adverse incidents.

2.1.3 FC Overview

The formation of FCs resulted from the events of September 11, 2001, and the need, identified by the 9-11 Commission, to close the information-sharing gaps that have existed between the Federal government and States, primarily in the areas of homeland security and law enforcement. Missions among FCs vary and include, but are not limited to, three main areas—all-crimes, all-hazards, and counterterrorism, as presented in Table 2-2.

Table 2-2: FC Mission Areas

All Crimes	Any crime or investigative support related to a single criminal act or larger criminal enterprises and organized or destabilizing crimes (e.g., drug trade, gangs, terrorism, and organized crime).
All Hazards	Identifying and prioritizing types of major disasters and emergencies, beyond terrorism and crime that could occur within their jurisdiction. For this approach, fusion centers gather, analyze, and disseminate information that would assist the relevant responsible agencies (law enforcement, fire, public health, emergency management, critical infrastructure, etc.) with the prevention, protection, response, or recovery efforts of those incidents.[7]
Counterterrorism	Practice, tactics, techniques, and strategies adopted to prevent or mitigate specific terrorist acts.

7 Federal Emergency Management Agency, *Draft Comprehensive Preparedness Guide 502: Considerations for Fusion Center and Emergency Operations Center Coordination*, 2009, page 14.

The *Baseline Capabilities for State and Major Urban Area Fusion Centers* outlines the major functional, management, and administrative capabilities of FCs. Fusion process capabilities outline the standards necessary to perform the steps of the Intelligence Process within an FC. Management and administrative capabilities enable the proper management and functioning of an FC. Table 2-3 shows the specific capabilities for each type.[8]

Table 2-3: FC Baseline Capabilities

Fusion Process Capabilities	
Planning and Requirements Development	• Lay the foundation for the types of information that will be collected
Information Gathering/Collection and Recognition of Indicators and Warnings	• Develop and implement planning and requirements • Collect information from various sources, including law enforcement agencies, public safety agencies, and the private sector
Processing and Collation of Information	• Evaluate the information's validity and reliability • Collate information, including sorting, combining, categorizing, and arranging the data collected so relationships can be determined
Intelligence Analysis and Production	• Transform the raw data into products that are useful • Develop a report that connects information in a logical and meaningful manner to produce an intelligence report that contains valid judgments based on analyzed information, including trends or information that will prevent a terrorist attack or other criminal activity
Intelligence/Information Dissemination	• Distribute analyzed intelligence utilizing certain protocols in the most appropriate format to those in need of the information to facilitate their accomplishment of organizational goals
Reevaluation	• Assess current and new information, assist in developing an awareness of possible weak areas as well as potential threats • Strive to eliminate previously identified weaknesses that have been hardened as a result of the Fusion Process • Provide an opportunity to review the performance or effectiveness of the FC's intelligence function
Management and Administrative Capabilities	
Management/Governance	• Develop clear priorities and create a supported environment that frames the ability for the center to function and operate, assign tasks, allocate and manage resources, and develop and enforce policy

8 U.S. Department of Justice, *Baseline Capabilities for State and Major Urban Area Fusion Centers: A Supplement to the Fusion Center Guidelines*, September 2008.

Information Privacy Protections	• Develop, publish, and adhere to a privacy and civil liberties policy • Protect the rights of Americans throughout information-sharing efforts • Balance information sharing with privacy at all levels of government, in order to maintain the trust of the American people
Security	• Ensure appropriate security measures are in place for the facility, data, and personnel
Personnel and Training	• Achieve a diversified representation of personnel based on the needs and functions of the center
Information Technology/ Communications Infrastructure, Systems, Equipment, Facility, and Physical Infrastructure	• Integrate technology, systems, and people
Funding	• Establish and maintain the center based on funding availability and sustainability

According to the Government Accountability Office (GAO), the most frequently cited reason for establishing an FC was the need to share information among Federal, State, and local entities. At the State and local level, the enhancement of information sharing within their own jurisdictions and across the various disciplines was another reason for the establishment of centers.[9] The inability for coordination and information sharing at these two levels resulted in a failure to "connect the dots" prior to September 11, 2001. Today, FCs consider themselves force multipliers to, and a support structure for, existing EOCs, which have the main responsibility of response during large-scale incidents and disasters, either man-made or natural.[10] Because some incidents may have components that are law enforcement or security sensitive, some EOCs have taken extra steps to ensure they have people on staff with appropriate clearances to review such information. They may also have developed methods for handling such data such as a secure communications system and designating a part of their facility to meet the National Security Agency's requirements of a Sensitive Compartmented Information Facility (SCIF).

2.2 Statistics, Locations, Jurisdictions

Each type of center manages a distinctive footprint in terms of size, geographic area, population served, and physical characteristics. This section defines the census and geographic distribution of each center and categorizes the types and jurisdictions of the various centers.

9 U.S. Department of Homeland Security, *National Incident Management System*, March 1, 2004, page 129.

10 Government Accountability Office, *Homeland Security: Federal Efforts are Helping to Address Some Challenges Faced by State and Local Fusion Centers*, April 2007.

2.2.1 TMCs

TMCs are regional information management centers that gather and maintain transportation-related data. Across the United States, over 100 TMCs currently leverage their ITS resources to monitor, inform, and control drivers in a localized region. Each center has unique applications, resources, size, and functionality. State departments of transportation (DOTs), county and city governments, or other municipalities, often collaborating with other agencies and each center, can fund and operate such centers.

The TMC footprint can be categorized primarily by urban or rural geographies. A variety of sources identified at least 85 TMCS as operating in metropolitan areas. In 2004, there were 50 additional TMCs providing a range of transportation-related services in statewide/rural capacity.[11] Table 2-4 defines the distinctions in these types of TMCs. It is also important to note that TMCs can be virtual in nature.

Table 2-4: Urban vs. Rural TMCs

Urban	Urban TMCs often focus on freeways and traffic signal management and possibly transit operations integration, with their key function revolving around the detection, response, and management of traffic incidents to keep traffic moving. They are frequently larger in size and more developed because of their substantial resources and funding. Because they have been operating longer, they have had the opportunity to establish working relationships with other agencies, including taking advantage of co-located facilities. Staff and management at urban TMCs often have specific job categories and responsibilities. Many TMCs in larger urban areas are integrating CAD and liaisons with local law enforcement to become immediately aware of police dispatches to an incident scene on a highway.
Rural	Rural TMCs are often much smaller and have fewer resources accessible to them, even though they are often responsible for a wider geographic area. Without an expansive ITS infrastructure, they focus on emergency services and rural transit service. Their smaller size results in a smaller, less-specialized staff and managers.

As each region faces different transportation issues, TMCs' mission and goals correlate to the needs of a local region. TMCs do not typically exist in more rural areas or on tribal lands due to the lack of traffic congestion and a lack of technology resources such as fiber optic networks by which to share data and information. Some states, such as New Mexico, coordinate with tribal lands on ITS projects. TMCs may serve larger geographic boundaries including cities and metropolitan areas, regions, municipalities, or States. Appendix B provides a listing of major TMCs.

2.2.2 EOCs

EOCs are the "front line" of incident response. By necessity, their reach must extend sufficiently to provide an immediate response to the affected areas within their jurisdictions. At least one EOC covers a jurisdiction, with smaller jurisdictions most likely sharing an EOC and larger jurisdictions having multiple EOCs. Tribal lands may also have EOCs that are eligible

11 U.S. Department of Transportation, *ITS Deployment Statistics*, 2004, http://www.itsdeployment.its.dot.gov, accessed 2010.

for funding through the DHS. In the case of a small or sparsely populated State, the State EOC may cover every jurisdiction (cities, counties, or other jurisdictional entities) within that State. In contrast, a densely populated State with densely populated cities may have other EOCs in addition to the State EOC.

Every jurisdiction is covered by an EOC (or a combination of EOCs) that addresses the full array of functional disciplines. For example, a small city may not have its own EOC; however, it may have a fire station that fulfills the EOC function for response to a limited type of incident (e.g., fires and similar emergencies within the jurisdiction), with other functional disciplines being covered by a shared EOC (e.g., a county, State, or regional EOC that responds to hurricanes, floods, and earthquakes across the broader jurisdiction). Table 2-5 illustrates the various types and numbers of governmental jurisdictions across the United States and its territories, commonwealths, and possessions.

Table 2-5: Governmental Jurisdictions[12]

Type	Number
States	50
U.S. Territories (3), Commonwealths (2), and Possessions (6)[13]	11
Counties or County Equivalents[14]	3,141
Cities (population 25,000 or more)[15]	1,248
Other[16] (incorporated places with populations less than 25,000)	18,161
Total	22,611

EOCs fall into three general geographic footprints, as presented in Table 2-6.

12 U.S. Census Bureau, *County and City Data Book*, 2007, http://www.census.gov/prod/2008pubs/07ccdb/ccdb-07.pdf, accessed 2010.

13 R.G. Price, "Territories, Possessions, and Influenced Areas of the United States of America," 2003, http://rationalrevolution.net/articles/territories.htm, accessed 2010.

14 The primary political divisions of most States are termed "counties." In Louisiana, these divisions are known as "parishes." In Alaska, which has no counties, the county equivalents are the organized "boroughs" and the "census areas" that are delineated for statistical purposes by the State of Alaska and the U.S. Census Bureau. In four States (Maryland, Missouri, Nevada, and Virginia), there are one or more cities that are independent of any county organization and, thus, constitute primary divisions of their States. These cities are known as "independent cities" and are treated as equivalent to counties for statistical purposes. The District of Columbia has no primary divisions, and the entire area is considered equivalent to a county for statistical purposes [*County and City Data Book*, 2007].

15 The term "city" refers to incorporated places with a 2000 population of 25,000 or more [*County and City Data Book*, 2007]. The number of cities was obtained from the 2002 Census of Governments, Volume 1, Number 1, Government Organization, DC: U.S. Department of Commerce, Bureau of the Census, as provided by the National League of Cities [http://www.nlc.org/about_cities/cities101.aspx].

16 The number of incorporated places with a 2000 population of under 25,000 was obtained from the 2002 Census of Governments, Volume 1, Number 1, Government Organization, DC: U.S. Department of Commerce, Bureau of the Census, as provided by the National League of Cities [http://www.nlc.org/about_cities/cities101.aspx].

Table 2-6: EOC Categories

Jurisdiction	Characteristics
Local Community EOC	• Continuously staffed and ready to respond to routine incidents affecting a limited jurisdiction (e.g., medical emergencies, fires) • Resources typically funded and controlled by the jurisdiction • Becomes a virtual component of EOCs with more extensive geographical jurisdictions when the impact of an incident extends beyond the local community (e.g., a hurricane)
State/ Metropolitan EOCs	• May be minimally staffed (e.g., a single watch officer on duty 24/7), with a surge capability when an incident warrants response • May directly own/control minimal resources but response involves coordinating resources typically funded and controlled by local community EOCs and/or other Federal or State entities • Jurisdiction is broader than that of a local community EOC, covering a densely populated or extensive geographic area
Federal EOCs	• Watch function may be more robustly staffed than State/metropolitan EOCs, but surge capability is triggered by incidents that may impact: – An extensive geographic area where response requirements exceed the response capability of local community and State/metropolitan EOCs and the State provides a request for Federal resources; or – National emergency, including security threats or incidents • Funded by Federal sources, but also coordinates resources funded and controlled by local community or State/metropolitan EOCs • May focus on a single functional area (e.g., response tailored to nuclear incidents or to incidents causing widespread, high-impact telecommunications service outages, such as the National Communications System's National Coordinating Center for Telecommunications within the Department of Homeland Security) • Jurisdiction covers the entire United States, its territories, and tribal nations

In addition to these State and local EOCs, there are also EOCs at the Federal level including the National Response Coordination Center (NRCC) at the Federal Emergency Management Agency (FEMA). According to the National Response Framework (NRF), the NRCC is a multi-agency center that provides overall Federal response coordination for Incidents of National Significance and emergency management program implementation. In addition, the NRF envisions Federal-level EOCs being established when a large-scale incident requires the establishment of such a temporary EOC to manage the response activities.

2.2.3 FCs

Research suggests that there are significant differences among FCs and that, heretofore, there was no "one-size-fits-all" model, despite the issuance of the FC guidelines in January 2008 by the U.S. Department of Justice (DOJ) and U.S. Department of Homeland Security (DHS). The *Baseline Capabilities for State and Major Urban Area Fusion Centers* document released in September 2008 provides supplemental guidance to the centers on standardized capabilities. As of July 2009, DHS and DOJ recognize 72 FCs nationwide, and the DHS

Office of Intelligence and Analysis (I&A) has deployed over 36 intelligence operations specialists to the FCs to facilitate the two-way sharing of information and intelligence and to bridge the gap in information sharing among Federal, State, local, territorial, and tribal levels of government.[17] In September 2009, DHS Secretary Janet Napolitano announced a realignment of I&A to create a new Joint Fusion Center Program Management Office (JFC-PMO) to strengthen DHS cooperation with FCs.[18] Appendix B provides a partial list of these centers and the functions they support.

The level of Federal, State, and local participation varies from FC to FC. The jurisdiction of an FC is limited only by the State or region that it serves. Jurisdictional cooperation between State FCs or between State FCs and Regional Intelligence Centers (RICs) provides an opportunity for information sharing to a level only imagined a decade ago. RICs are defined as "multi-jurisdictional centers cooperatively developed within a logical geographical area that coordinate Federal, State, and local law enforcement information with other information sources to track and assess criminal and terrorist threats that are operating in or interacting with the region."[19] Statistically, law enforcement agencies lead the day-to-day operations of most FCs. Of those law enforcement entities involved in FC operations, State police are often cited as the main organization spearheading their efforts. However, since FCs vary in location and mission, the lines that determine a lead agency are not as clear as the desire for participating agencies to be partners in their mission.

2.3 Processes and Operations

This section provides insights into the day-to-day functions, processes, and operations as well as emergency modes across TMCs, EOCs, and FCs.

2.3.1 TMCs

Generally, full-scale TMC operations focus on four primary function classifications:

- **Monitor**: Monitoring transportation infrastructure for traffic incidents/conditions
- **Inform**: Disseminating information to the public and relevant agencies
- **Control**: Controlling and managing traffic including optimization of available infrastructure and assets, such as safety/service patrols, to decrease congestion and mitigate incidents
- **Indirect**: Managing overhead activities for the TMC.

17 See U.S. Department of Homeland Security, State and Local Fusion Centers, http://www.dhs.gov/files/programs/gc_1156877184684.shtm, accessed 2010.

18 See Testimony of Secretary Napolitano before the Senate Committee on Homeland Security and Governmental Affairs, "Eight Years after 9/11: Confronting the Terrorist Threat to the Homeland" (Written Testimony), September 30, 2009, http://www.dhs.gov/ynews/testimony/testimony_1254321524430.shtm, accessed 2010.

19 *Baseline Capabilities for State and Major Urban Area Fusion Centers*, September 2008.

Across TMCs, these functions vary in terms of the extent to which and how they provide these services. Table 2-7 presents aspects of the incidents monitored, systems leveraged, and processes and operations of the TMC, revolving around the four primary functions.

Table 2-7: TMC Traffic Management

Incidents Monitored	Technologies and Tools Utilized	Actions
Relevant road-weather data	Automated roadway detection including road weather information systems (RWIS)	Broadcast of warnings and instructions if necessary Permanent fixed-route evacuation signing (in some areas)
Incidents	Cell phone calls to local law enforcement and 911 dispatchers, closed-circuit television (CCTV), CAD, and similar systems	Incident responder deployment including fire, police, paramedics, and/or safety/service patrols
Congestion	CCTV, loop detectors, vehicle probes	Dynamic message signs (DMS), also known as variable message signs (VMS) or changeable message signs (CMS), display appropriate messages providing travel time or congestion-level messages
Work zones	CCTV, radio and cellular communication with road crews Monitoring sensors in barrels or cones Intrusion alert devices	DMS display appropriate messages providing travel time Detour routes implemented and instructions provided as necessary Real-time monitoring of speeds around work zones and intrusion into a work zone
Special events	CCTV, signal timing adjustments, radio and cellular communications with State DOT field staff	Monitoring of special events and work with law enforcement to direct traffic as necessary
Signal timing	CCTV, Advanced Traffic Management Systems (ATMS), traffic signal algorithms	Monitoring of traffic including intersection movement, adjustment of signal times for optimal traffic flow

2.3.2 EOCs

At the most fundamental level, EOCs perform five primary functions and one administrative function—monitoring the jurisdiction, receiving notification of an incident affecting the jurisdiction, assessing the incident to determine the appropriate response, responding to the incident, closing out the incident, and administering the organization. The jurisdiction's emergency management plan defines who operates the EOC and how it is operated. At the Federal level, the NRF serves this purpose. EOCs are often organized around operations, planning, logistics, finance, and administrative departments—key Incident Command

System (ICS) organizational elements—to fulfill the basic EOC functions. EOCs establish processes required to fulfill the five primary EOC functions and document the processes in standard operating procedures (SOPs). The SOPs define how the operations, planning, logistics, finance, and administration components interact and how the EOC as a whole works with external entities (e.g., Federal, State, and local government entities and the private sector). Table 2-8 provides a sample of the processes defined by the EOC SOPs and the EOC functions with which these processes are associated.

Table 2-8: Illustrative EOC Functions and Processes

Functions	Processes
Monitoring	• Maintain steady-state watch • Monitor radio frequencies and CAD systems for police and fire departments • Survey all 911 calls and emergency response units • Track weather conditions • Monitor news media (e.g., CNN, MSNBC) • Monitor status of emergency response teams and resources
Incident Assessment	• Prioritize objectives • Make recommendations to government executives on evacuations, closures, disaster declaration, cessation of services
Incident Response	• Obtain resources • Deploy resources • Coordinate with other agencies and organizations • Assign tasks to Emergency Support Functions (ESFs) • Brief staff • Update government officials • Update news media (e.g., local/national news organizations)
Incident Closure	• Develop after-action reports for incident and/or exercise
EOC Administration	• Track time and costs of incident • Analyze data • Develop, maintain, and update action plans • Maintain duty log • Manage and train response personnel • Manage resource inventory (e.g., medical supplies) • Maintain equipment (e.g., vehicles, backup generators) • Provide administrative and legal support • Update Memorandums of Understanding (MOUs) and Memorandums of Agreement (MOAs) with neighboring jurisdictions and internal organizations

Note that, particularly in more widespread, complex incidents, these functions may be iterative and overlapping, rather than sequential and discrete. This is particularly the case with the monitoring, assessment, and response functions. Further, EOCs work closely with local

community resources frequently to manage incidents. The community owns monitoring and response resources and assets, which may include:

- E-911 call centers
- Local law enforcement agencies (to include law enforcement personnel, facilities, vehicles, etc.)
- Fire stations (to include firefighters, associated EMS personnel, facilities, and specialized vehicles such as ambulances).

However, EOCs with more extensive jurisdictions may own some facilities and have a few key staff, but they usually coordinate the monitoring and response resources rather than own them. EOCs are dynamic organizations depending on their operating status. During the watch or monitoring stage, the operating staff is minimal. During a full-scale operation, EOCs house representatives from multiple agencies and organizations ranging from executive government officials to volunteer organization coordinators.

In contrast with the local community-level response entities, whose fire departments, law enforcement agencies, and medical organizations are in continuous operation, EOCs with more extensive jurisdictions typically have a small core staff on duty until an incident occurs that requires activating the EOC's full capabilities. In some cases, "core staff" may be limited to having a single watch officer on duty on a 24/7 basis.

2.3.3 FCs

FC guidelines state that the principal role of the FC is to compile, analyze, and disseminate criminal and terrorist information and intelligence and other information to support efforts to anticipate, identify, prevent, and/or monitor criminal and terrorist activity.[20] FCs leverage all information and intelligence to rapidly identify patterns and trends that may reflect emerging threats. The primary functions and goals for FCs, as defined by the guidelines, are to:

- Rapidly identify emerging threats
- Support multidisciplinary, proactive, and community-focused problem-solving activities
- Support predictive analysis capabilities
- Improve the delivery of emergency and non-emergency services.

Of these activities, the primary function of an FC is to gather and analyze data, resulting in a finished, timely, credible, and actionable product that is useable in the decision-making process.

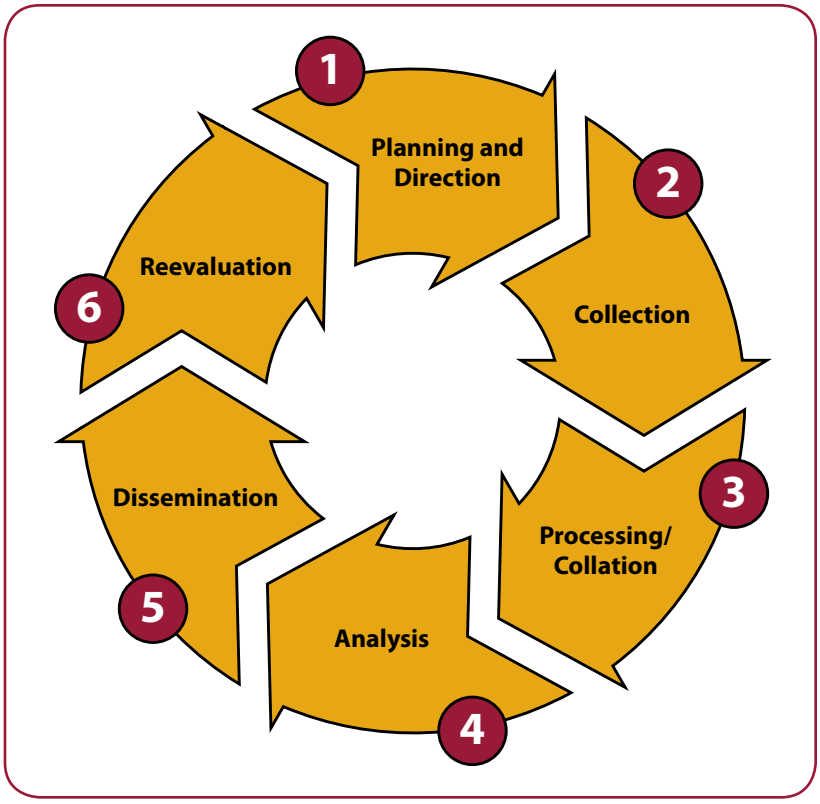
When a threat is identified, FCs gather and exchange information from all sources for analysis with the appropriate official from the local, State, tribal, or Federal government agency represented at that FC, based upon the threat. While law enforcement or homeland security sources and databases or portals provide nearly all intelligence and information that FCs

20 *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*, January 2008.

collect, agencies external to law enforcement, such as transportation agencies, fire departments, private sector, and public health entities, may also provide critical information to formulate a comprehensive analysis.[21] Depending on the nature of the threat, the FCs may share this threat information with DHS and, when terrorism related, coordinate with Joint Terrorism Task Forces (JTTFs) that exist in 100 cities nationwide including the Federal Bureau of Investigation's (FBI's) 56 field offices.

The local, State, tribal, or Federal government representative that will be taking action against the threat stores the products produced by an FC, based on the specific threat. Storing of that product is done in accordance with any FC and/or department policy, to include local, State, and Federal classified information requirements and privacy laws.[22] Figure 2-1 illustrates the FC intelligence process.

Figure 2-1: FC Intelligence Process[23]



2.4 System Capabilities and Resources

Defining the systems capabilities and resources for TMCs, EOCs, and FCs is a key element to understanding the opportunities for collaboration across these entities. This section sum-

21 *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*, January 2008.

22 Ibid.

23 Source: U.S. Department of Justice, *The National Criminal Intelligence Sharing Plan*, October 2003. http://it.ojp.gov/documents/NCISP_Plan.pdf, accessed 2010.

marizes the resources and systems that enable each center to fulfill its core functions and processes as defined in previous sections.

2.4.1 TMCs

TMCs maintain specific resources and systems to enable the fulfillment of their four primary functions. Monitoring arterial and freeway traffic is one of the primary functions of TMCs. Only with situational awareness of local conditions can TMC managers make decisions on how to increase transportation safety and throughput. ITS applications that are installed in the transportation infrastructure, including traffic sensor systems to monitor traffic conditions perform much of the surveillance and detection of traffic conditions.

In addition to monitoring transportation infrastructure for traffic management functions, the same surveillance and detection technologies can be used to monitor the infrastructure safety and security of transportation infrastructure. Table 2-9 provides examples of monitoring systems.

Table 2-9: TMC *Monitor* Systems and Resources

Description	Systems/Resources
Monitor Traffic	Loop, acoustic, radar, and video imaging detectors and control, CCTV, IntelliDrive℠, on-board equipment (OBE), wide-area wireless communications between the vehicle and center, dedicated short-range communications (DSRC) between passing vehicles and the roadside, probe data (cellular, Global Positioning System [GPS], toll transponders), police reports (incidents and congestion)
Monitor Safety and Security	In-vehicle and facility surveillance, employee credentialing, remote video systems, speed sensors, safety/service patrols

After collection of information regarding a traffic incident and decision making regarding the appropriate actions and responses, TMCs disseminate traffic information to system users to inform them of conditions and possible actions. Information can be disseminated to users both before and during driving, as illustrated in Table 2-10.

Table 2-10: TMC *Inform* Systems and Resources

Description	Systems/Resources
Disseminate Information	DMS (fixed and portable); in-vehicle systems; Highway Advisory Radio (HAR)/Low Power FM (LPFM); 511/Voice Response Phone Systems; 511 Web Portals (real-time traffic maps); email, pager, fax, short message service (SMS)
Implement Road Geometry Warning Systems	Ramp rollover, curve speed warning, downhill speed warning, overheight/ overwidth warning

Table 2-11 presents how TMCs employ the information gathered to control traffic and manage incidents and ongoing activities that impact traffic on a daily basis.

Table 2-11: TMC *Control* Systems and Resources

Description	Systems/Resources
Control Traffic	Transit signal priority, emergency vehicle preemption, adaptive signal control, advanced signal systems, variable speed limits, lane use/road closure, vehicle restrictions
Manage Lanes	High occupancy vehicle/high occupancy toll (HOV/HOT) facilities, reversible flow lanes, pricing, lane control, variable speed limits, DMS (fixed and portable), emergency evacuation
Control Ramps	Ramp metering, ramp gates, interchange metering, priority access
Incident Management	Safety/service patrols, CCTV, police reports of incidents and congestion, CAD, access restriction and authentication, firewalls, antivirus and network monitoring software, physical barriers
Manage Work Zones	Temporary traffic and incident management, lane control, variable speed limit, speed enforcement, intrusion detection, road closure management
Manage Special Event Transportation	Occasional and frequent events, temporary TMCs, automatic vehicle location (AVL)
Manage Transportation Demand	Ride sharing/matching, dynamic routing and scheduling, service coordination, pricing
Manage Assets	Fleet and infrastructure management
Manage Electronic Tolling and Pricing (tolling; transit, parking, and multi-use)	Radio frequency identification (RFID), barcodes, smart cards
Facilitate Evacuation Response and Recovery	Early warning system, response management, evacuation and re-entry management
Coordinate EMS	Telemedicine, 911 coordination

To tie together their other direct functions, TMC staff also manage communications among their operations center, the infrastructure, mobile responders (e.g., safety/service patrols), and other relevant agencies and operations centers. This requires TMCs to have access to all necessary communications links and to develop integrated control strategies that enable inter-jurisdictional traffic management. TMCs' communications include land and wireless technologies as well as digital and hard lines. Additionally, it is also important to note that TMCs must plan for remaining functions in emergency and disaster situations. Local weather alert and warning systems, such as the National Warning System (NAWAS) and the Tsunami Warning System (TWS), used by EOCs or FCs could give TMCs critical real-time weather alert information on dangerous weather in an area, thus allowing TMCs to better prepare for these emergencies. When faced with such situations, TMCs must implement and install system redundancies to ensure that their systems stay online during an incident. Table 2-12 presents systems and resources that support the indirect functions of a TMC.

Table 2-12: TMC *Indirect Functions* Systems and Resources

Description	Systems/Resources
Coordination of Communications	Additional communications links and integrated control strategies that enable integrated inter-jurisdictional traffic management, phone systems, (e.g., land line, special 1-800 call-in lines, conference call lines), mobile and satellite phones, dedicated lines, priority telephone services—Wireless Priority Service (WPS), priority cellular services—Government Emergency Telecommunications Service (GETS), push-to-talk services, email/text messaging, personal data assistants (PDAs), pagers, radio communications system (center-to-field, field-to-field, field-to-center), PCs/laptops, Internet
Redundancies	Back-up servers and facilities
Security	Encryption software, access restriction and authentication (username and passwords), firewalls, antivirus and network monitoring software, physical barriers (e.g., fence, spike strips, electronic locks)

2.4.2 EOCs

An EOC often functions as the hub of emergency management in a community and, in some instances, is co-located with an FC, ensuring that resources are available to respond to a full array of incidents:

- On a day-to-day basis, some EOCs oversee the response to routine incidents (e.g., a fire or an automobile crash) and are generally self-sufficient with respect to their resources. For example, EOC staff and the emergency management offices may own vehicles (e.g., fire trucks and ambulances) and hire employees (e.g., firefighters, police, or emergency medical technicians [EMTs]), or these may be the resources of law enforcement or fire departments.
- When incidents occur that affect a broader geographical area (e.g., a hurricane) or are non-routine (e.g., a chemical spill), the community EOCs seek assistance from an EOC with either a broader geographical jurisdiction or an EOC that may have specialized capabilities to respond to incidents that are not part of the EOC's day-to-day area of responsibility. In such cases, the community EOC may function as a component of the higher-level or specialized EOC for the duration of the incident, and its resources may be augmented by those of other organizations such as State or Federal government or non-government organizations (e.g., the Red Cross).

As is the case for an EOC's operating status or its functional organization, the resources available to an EOC depend on a community's individual needs and investment in preparedness, perceived risks, emergency management, and public safety capabilities. With respect to technologies for managing their resources and information, EOCs do not typically have access to specialized technologies. Certain factors mitigate the availability of specialized technologies in EOCs. In many cases, EOC 24/7 staffing constitutes a single watch officer on duty at any given time. The EOC is fully activated only when a significant situation arises that warrants a response. Consequently, highly specialized technologies would be used only intermittently, and the cost-per-use may be prohibitive. Further, if such technologies are not used routinely, there is no opportunity for the staff to become sufficiently profi-

cient with them to warrant the expense. It may even impede response if EOC staff members had to re-acquaint themselves with the technology every time the EOC is activated.

More often, EOCs rely on output from the systems owned and operated by other agencies or use technology that is available to most citizens, including, for example:

- **Output from other agencies' systems**: EOCs benefit from technologies operated by other agencies because those agencies have staff that are familiar with the technologies and can provide useful output to the EOCs. This allows the EOCs to benefit from these systems without having to invest their limited resources in them. Modeling tools represent the type of technology borrowed by the EOC as needed.
- **Radio and TV**: EOCs use information available via radio and TV, which in most cases offers up-to-the-minute information on breaking situations, again without requiring the EOCs to expend any resources on such information.
- **Internet**: Internet access allows EOCs to access information available to the general public, such as the weather reports provided by the National Oceanic and Atmospheric Administration's (NOAA's) National Weather Service (NWS). This is also a method for accessing information generated by the technology owned and operated by other agencies.

Although the commonly available technologies such as radio, TV, and the Internet may not be tailored to the EOCs' requirements, they provide valuable information without incurring expense and requiring continuous training on the technologies. There are some EOCs that have more advanced technologies. These are generally the EOCs for jurisdictions with high populations or that have significant strategic importance, such as those having high-traffic ports or key government facilities. Examples of more advanced technologies used by EOCs include software programs (e.g., Geographic Information System [GIS]), warning systems, videoconferencing equipment to coordinate with external responders to receive real-time damage estimation, and specialized encryption and security communication areas.

Warning systems such as NAWAS are networks of telephone lines used by emergency personnel for coordination and response to natural and man-made disasters. The lines avoid local telephone switches to avoid congestion during an emergency. Both of these warning systems are based on human intervention and can easily be linked to TMCs (e.g., call forwarding, conference calls, and party lines). One of the benefits of this linkage would be near instantaneous information on dangerous weather approaching an area, which the TMC could then use to notify the driving public and place emergency road crews on standby.

2.4.3 FCs

Many FCs have access to unclassified and classified DHS and FBI systems and networks such as HSIN, Law Enforcement Online (LEO), and Homeland Security Data Network (HSDN). HSIN is an encrypted DHS network established to strengthen the real-time, collaborative flow of threat information to State and local communities.[24] HSIN links to DHS' National Operations

24 U.S. Department of Homeland Security, *Fact Sheet: Homeland Security Information Network*, 2004, http://www.dhs.gov/xnews/releases/press_release_0418.shtm, accessed 2010.

Center (NOC) via the Joint Regional Information Exchange System (JRIES), which is also a secure network that offers FC applications including imaging and mapping resources.

Information for FCs is usually gathered through law enforcement or homeland security sources, i.e., LEO and HSIN, but also draws from the emergency management and functional communities (e.g., transportation, health and human services). The agencies that operate within the FCs are able to operate as long as secure portal access is available to them from their home agency. DHS/I&A intelligence operations specialists are deployed to the FCs with both unclassified and classified systems.

Problems are usually encountered when FCs without a specific Federal, State, local, or tribal representative in their center are unable to access some specific piece of information that they need from that State, local, or tribal jurisdiction. This often results if the right people do not have necessary clearances and a need to know. In many cases where the information is of an unclassified nature, there are other avenues, a phone call for example, to obtain the desired information.

2.5 Information Managed and Exchanged

An important aspect of establishing effective information exchange is integration and information sharing among partnering agencies to avoid inefficient exchanges of information. Establishing a system includes defining the data for exchange and compensating for any differences in how agencies code their data, including data fields, abbreviations, or summary methodologies. Each agency must account for the available incoming information for exchange with other agencies, considering the information that is of interest to each agency as well as security. Coordination must also occur with software and hardware vendors to ensure that linked systems are able to still share information after updates and so that software release schedules are coordinated with agency project schedules. Also, while data duplication should be minimized to decrease redundancy, redundant communications paths are necessary to ensure the reliable delivery of messages during incidents.

2.5.1 TMCs

TMCs gather real-time information and data with a key focus on near-term regional operational transportation information including proactive steps to manage congestion and other bottlenecks. Table 2-13 summarizes the types of traffic data collected and the resources used to acquire the data.

Table 2-13: TMC Data Types and Sources

Data Type	Source
Traffic Speed	• Loop Detectors and Control • Acoustic Detectors and Control • Probe Data – Cellular, GPS, E-ZPass • Radar Detectors and Control including iCone in work zones • Video Imaging Detectors and Control • Models and algorithms to enhance traffic information • In-Vehicle Systems
Travel Time	• Probe Data – Cellular, GPS, E-ZPass • Models and algorithms to enhance traffic information
Traffic Incidents	• In-Vehicle Systems • HAR • DMS (fixed and portable) • 511/Voice Response Phone Systems • Safety/Service Patrols • Police Reporting of Incidents and Congestion • Police Dispatch • CCTV
Delays and Congestion	• Adaptive Signal Control • In-Vehicle Systems • HAR • DMS (fixed and portable) • 511/Voice Response Phone Systems • Safety/Service Patrols • Police Reporting of Incidents and Congestion • CCTV
Traffic Volume	• Loop Detectors and Control • Radar Detectors and Control • Video Imaging Detectors and Control • Adaptive Signal Control
Roadway Weather	• 511/Voice Response Phone Systems • Surface sensors and roadside weather stations
Work Zones	• DMS (fixed and portable) • HAR

The main commodity that TMCs offer is information regarding local traffic conditions and incidents that affect them. They are responsible for three types of transportation-related information:

- Operational information including real-time situational information on the transportation infrastructure

- History and records information including incident logs and traffic/transportation history
- Transportation network information including information about physical transportation-related assets.

TMCs can disseminate collected and owned information to the public via:

- **Dynamic Message Signs (DMS)** – Roadside signs with a communications link to the TMC that the TMC can use to display short–route messages to system users including emergency information such as evacuation shelter locations or AMBER Alerts™ with child abduction information and Silver alerts providing information on missing senior citizens.
- **Highway Advisory Radio (HAR) and Low-Power FM Radio** – Low-power radio stations that TMCs use to provide traffic and weather updates, advertised via roadside signs.
- **In-Vehicle Communications** – New technologies (IntelliDrive^{SM}) allowing new methods for TMCs to communicate directly with drivers in their vehicles.
- **511 Traveler Information Systems** – 511 is the Federal Communications Commission's designated nationwide three-digit telephone number for traveler information. It is usually an automated hotline, although some 511 systems are staffed with live operators, providing an automated phone message (sometimes multi-lingual) to system users regarding local traffic or weather conditions. Some 511 systems allow users to also access information via a Web site, and some feature personalized services such as custom routes and alerts via phone, text, or e-mail. The 511 system can be used to provide emergency information (e.g., evacuation route information) via a floodgate message at the start of the 511 recorded message to all callers. According to the 511 Deployment Coalition, as of the end of 2009, 511 will be accessible to 70 percent of the U.S. population.[25]

  In addition to outgoing information, 511 systems could be modified to handle incoming information from the public. A few 511 systems have implemented this option for key personnel but not the general public. For example, if someone witnesses a vehicle crash, he/she could dial 511 on a cell phone and be presented with two options. Option 1 would be to listen to current traffic information and advisories, and option 2 could be re-routing the call to a statewide or the nearest TMC. Current applications require the user to provide a personal identification number so the TMC knows the information is coming from a trusted source. The caller can then record a message with the relevant information. The call is then automatically routed to the TMC. The routing could use information given by the caller (e.g., highway name and mile marker) as well as cell phone data (e.g., approximate location data based on cell-tower triangulation) to provide proper routing. Once the TMC has received the message, operators can verify it, notify emergency response personnel and cleanup crews, and update the 511 outgoing information line. If the incident meets a certain threshold (e.g., size, duration), the TMC could route the information to the EOC and FC.

25 U.S. Department of Homeland Security, *Fact Sheet: Homeland Security Information Network*, 2004, http://www.dhs.gov/xnews/releases/press_release_0418.shtm, accessed 2010.

- **Third-Party Communications –** Authorized dissemination of TMC-provided information (e.g., Traffic.com).

In addition to providing information to the public, TMCs can specifically collaborate with and exchange information with other State, local, and municipal agencies including EOCs, FCs, and law enforcement. In this way, TMCs can offer a valuable service by providing real-time situational awareness to other decision-making agencies and responders on the ground. Information collected by TMCs that may be exchanged with other agencies includes:

- Real-time video images provided with CCTV video feeds via access to a common portal or a direct video feed
- Traffic sensor data providing congestion information such as speed, volume, and travel time, shared via common Internet portal
- Weather sensor data providing regional, area, and surface condition data including temperature, pressure, and precipitation
- IntelliDrive[SM] on-board equipment (OBE) providing aggregate data from hundreds of vehicles including temperature, wiper status, anti-local brake system (ABS) status, and brake status among others
- IntelliDrive[SM]-based algorithms, such as "Icy Conditions," "Incidents," "Link Speed," "Travel Time," and "Volumes," providing near real-time information about road conditions and possible evacuation routes
- IntelliDrive[SM] Advisory Message Delivery System providing near instantaneous two-way communication with the driving public across vast areas
- Reverse 911 systems providing continuous updates to first responders, decision makers, and other members of the non-driving public
- Integrated Public Alert and Warning System (IPAWS) utilizing data from TMCs to alert the general public with life-saving information quickly
- Incident and congestion notifications providing location, cause, extent, time, detection, and clearance of incident and congestion via radio, fax, or phone (incident logs and network statistics are also available for historical information)
- Planned projects, work zone, and special events in-progress information including providing location, extent, time, and status via the Internet, radio, fax, or phone
- GPS and GIS data providing vehicle location and speed as well as special information from multiple sources via Internet portal
- Traffic control systems data providing information regarding the activity/inactivity and operational status of ramp meters, traffic signal control, lane control signals, and DMS content via common Internet portal

- Public transit systems data including passenger vehicle times, locations, trajectories, origins, and destinations
- CAD systems providing response information including incidents, dispatch information, and status via a linked software program that allows a computer to automatically dispatch emergency responders.

While much of this information can be collected and shared, agencies must be mindful of laws on sharing sensitive information. Typically 911 centers have access to law enforcement networks (e.g., the Virginia Criminal Information Network or the New York State Police Identification Network). These law enforcement databases provide police officers with access to motor vehicle license and registration information, wanted information, missing persons, stolen vehicles/articles, etc. Access to this data is tightly controlled and may be exempt from Federal and State information access laws and would not be shared outside of the law enforcement agency. Exemptions would be necessary for TMCs to receive only pertinent data related to their objectives.

Some data, like medical information and crash information have specific protection. For example, medical information falls under Health Insurance Portability and Accountability Act (HIPAA) regulations, while other personally identifiable information (PII) would come under the Privacy Act and other Federal or State and local protections. Crash data, such as data from passenger vehicle event data recorders and OnStar systems provide at least several dozen crash data elements (e.g., speed at time of a crash, whether a seat belt was in use), but may require a court order for access to the data. TMCs need an exemption to receive such data, after stripping of PII.

Data sharing between municipal agencies, working for the same local government, is easily accomplished. However, some city, State, and Federal laws prevent the release of data from one entity to another either entirely or partially but with built-in safeguards. There are many restrictions on data sharing at different levels. To accomplish efficient data sharing that respects individuals' rights, one has to look at how a particular entity intends to use that data.

- A driver's medical history may be of great importance to 911 call centers and first responders, but a TMC may not need that information.
- An explosion at a chemical plant would not concern a TMC, unless that plant was near a highway that would be impacted by the explosion.

There is a need for more data-sharing agreements between the State and these centers, especially FCs. It is best to have detailed agreements in place before the creation of an FC. One such agreement could provide for direct feeds of appropriately redacted data from 911 centers into the FCs.

As a result of recent concern about alleged racial and ethnic profiling in traffic stops, a number of law enforcement agencies (both local and State) now operate under policies requiring statistical review and audits of traffic stop and other police encounter data. Other agencies may want to review the results of those audits and evaluations to determine

whether anticipated information collection and enforcement initiatives are consistent with the findings of such oversight. Access to this data may require special requests because the analyses may not be covered by standard information-sharing agreements between and among law enforcement agencies.

2.5.2 EOCs

To support their coordinating role, many EOCs use information management tools, such as WebEOC®, to exchange information and prioritize requests during an incident. Availability of these information-sharing tools may be limited to personnel in the EOC or may be extended to the broader emergency response community, to include first responders in the field or TMCs. These information tools may include CAD and GIS mapping capabilities and are usually customized for individual EOCs.

Access to continuously updated information is critical to successful incident response. One important function is providing Situation Reports (SITREPs) every few hours during a major incident. Figure 2-2 shows a sample SITREP. SITREPs describe the situation on the ground, response priorities, and actions taken or underway to resolve the most urgent issues. Depending on the situation and the level of priority, SITREPs may include synthesized data provided by a TMC, such as a status report on a crash along a key evacuation route.

Figure 2-2: VEOC SITREP Extract

Virginia Emergency Operations Center (VEOC)
Virginia Department of Emergency Management (VDEM)
Virginia Emergency Response Team (VERT)

March 4 2008 TORNADOES
SITUATION REPORT # 13
14 April 2008, 1400 Hours

New information is in BOLD ITALICS.

SUMMARY

In the early evening hours of March 4 a cold front moving across the Commonwealth generated storm activity. These storms produced rain, wind and reported tornadoes. National Weather Service Morristown confirmed that an EF1 Tornado did touch down in Big Stone Gap, Wise County Virginia. Preliminary damage reports have been received from several jurisdictions and state agencies. No injuries or deaths were reported.

EXECUTIVE ACTION

EOC Activation:	The Virginia VEOC is at Recovery Operations with ***normal*** staffing.
State of Emergency:	Governor Kaine declared a State of Emergency at 1119 hours 5 March 2008. Executive Order – NUMBER SIXTY-FOUR (2008)
Federal Declaration:	No declaration has been requested at this time.
Protective Actions:	Local Emergency Declared by: Wise County at 1800 hours 4 March 2008 Town of Big Stone Gap at 1700 hours 4 March 2008 Essex County at 0800 hours 5 March 2008

WEATHER

Forecast:	**Southwest VA: Monday 14 April: *Mostly cloudy with rain showers likely; high temperatures in upper 30's to low 40's; north winds 10 to 15 MPH.* Monday night: *Mostly cloudy with slight chance of rain showers and snow showers in the evening and snow showers after midnight; patchy frost possible toward daybreak; low temperatures in the low 30's; north winds 5 to 10 MPH.* Tuesday 8 April: *Sunny; high temperatures upper 40s to low 50s; north winds 5 to 10 MPH.* Tuesday night: *Clear; low temperatures in low 30's; light and variable winds.***

OPERATIONS SECTION

ESF 5 – Emergency Management:	Virginia Department of Emergency Management (VDEM) Event created in WebEOC "2008-03 Tornadoes 03-04-08". VDEM and localities posting event related information and resource requests in WebEOC. VDEM is monitoring recovery operations.

This extract SITREP from the Virginia EOC (VEOC) includes transportation specific information following a series of tornadoes in April 2008. The full SITREP can be viewed at http://www.vdem.state.va.us/newsroom/sitreps/2008/mar4_tornadoes/sitrep13.pdf.

SITREPs can be tailored for particular audiences. For example, they may be designed to communicate with the general public, in the form of a press release, or they may be designed to communicate classified or otherwise sensitive information to law enforcement or military personnel during a terrorist incident.

Producing effective SITREPs and incident management plans requires EOCs to gather, analyze, and prioritize large quantities of data from a variety of sources. When representatives from different agencies are physically present in the EOC during an incident, they can serve as expert conduits of information to the lead EOC staff. For instance, the ESF-1[26] (transportation) representative usually coordinates the exchange of critical information between the EOC and the affected transportation agencies and providers. With advances in communications technologies, however, representatives can accomplish this objective remotely. Section 2.6.2 of this guidebook provides details on communications capabilities typical of EOCs. There are challenges associated with communications technologies as well; Section 4.2 of this guidebook discusses these.

EOCs are in the best position to help decision makers at the TMCs by providing them with useful and timely information. Integrating TMC information systems with information management and reporting systems such as WebEOC® and providing TMCs with SITREPs that go beyond the information included in press releases will greatly enhance TMC personnel's ability to deal with unplanned events. Regulatory and privacy concerns can be addressed by ensuring that the information shared with the TMC only includes aggregate data.

Table 2-14 reflects data and its sources coming into the EOCs, which they use to conduct their emergency operation functions (e.g., monitoring the jurisdiction, receiving notification of an incident affecting the jurisdiction, assessing the incident, responding to the incident, and closing out the incident).

Table 2-14: EOC Data Types and Sources

Data Type	Data Source
Weather	• Direct feed • Commercial broadcast media • Public Internet sites • GIS • Hard-copy maps • Public Internet sites • Remote sensing data and maps

26 ESF-1 is defined by FEMA as transportation assisting Federal agencies, State and local governmental entities, and voluntary organizations requiring transportation capacity to perform response missions following a major disaster or emergency. ESF -1 also serves as a coordination point between response operations and restoration of the transportation infrastructure.

Data Type	Data Source
Resource Deployment	• CAD • EOC staff • On-site responders • RFID and GIS technology • Resource tracking tools
Situational Status	• Commercial broadcast media • CAD • Police/fire radio traffic (911 dispatch) • TMCs/TOCs • EOC staff • On-site responders • General public • Remote sensing data and maps
Incident Response Plans	• Hard copy • LAN

2.5.3 FCs

Traditionally, information that FCs have managed and exchanged has been done through law enforcement and/or homeland security agencies. However, because many FCs have an All-Crimes or All-Hazards mission approach, they are engaging non-traditional information and intelligence sources for information management and exchange. Many FCs have developed a Fusion Liaison Officer (FLO) Program—a network of FC liaison officers who are members of law enforcement, fire service, public health, and other agencies (including public works, corrections, and emergency management). Several States have established these programs to facilitate communication with FC stakeholders, including law enforcement and emergency management. FLOs coordinate information-sharing activities among the private sector and CIKR partners, such as electric companies, oil refineries, banks, and entertainment facilities. With the help of this network, FCs receive homeland security and crime-related information for assessment and analysis.

The Homeland Security Act of 2002 and Presidential Executive Order 13356, issued on August 27, 2004, provided the impetus for a national effort to improve information sharing and defined the DHS' initial role in this effort.[27] This role has been expanded and refined in subsequent statutes, such as the Intelligence Reform and Terrorism Prevention Act of 2004, as amended (IRTPA).[28] IRTPA ensured that DHS would have a central part in the Information Sharing Environment (ISE).[29] FCs reported to the GAO that they issue a variety of products, such as:

- Daily bulletins on general crime and information

27 U.S. Department of Homeland Security, *Department of Homeland Security Information Sharing Strategy*, April 2008, http://www.dhs.gov/files/publications/gc_1212068752872.shtm, accessed 2010.

28 Ibid.

29 Ibid.

- Weekly bulletins on criminal or intelligence information
- Assessments for in-depth reporting on emerging threats, groups of interest, or crime.

To obtain daily information, FCs access databases from the Federal Trade Commission, DHS, US DOJ, the Office for the Program Manager for the ISE (appointed by the President), and even limited information from the Central Intelligence Agency (CIA). Each of these organizations has taken steps to provide FCs with access to Federal information systems. Appendix C of this report provides a listing of databases that the FCs may access.

DHS reports that, as of August 2009, the HSDN is deployed at 29 FCs. This communications network allows the Federal government to move information and intelligence to the States at the secret level. Through HSDN, FC staff can access the National Counterterrorism Center (NCTC), which is a classified portal of the most current terrorism-related information according to its Web site. Many FCs will have an SCIF where they have access to classified information, operated either by the FBI, DHS I&A, or other designated agencies. Collaborative network capabilities exist for the purposes of sharing information between the Regional Information Sharing Systems (RISS), LEO, and DHS' HSIN.

In many cases, concern over information management systems is due to the fact that State systems cannot work with other systems within the State or regionally since there is no single national-level system. Despite Federal efforts to promote the use of Extensible Markup Language (XML) as the standard format across all levels of government for justice and public safety information management systems, FCs and States continue to purchase systems that operate using proprietary language and that cannot "speak" to other systems without additional equipment and costs.[30] However, information sharing has been a long-standing practice among justice agencies, particularly within the law enforcement community according to FC guidelines.

FCs have been providing their partners with alerts, bulletins, reports, and assessments, all in an effort to improve the quality of information and the process of information sharing. In the beginning, most of the partners were Federal and law enforcement organizations. However, this has been evolving as the centers move toward an "All Hazards" approach. The intelligence alerts and bulletins serve to provide immediate information and updates, respectively, to present situational awareness and a clearer operating picture to first responders. Daily and intelligence reports look at larger regional and global issues. These reports serve to inform the recipients of trends or concerns in various sectors such as:

- Agriculture and food
- Banking and finance
- Hazardous materials (HazMat) and the chemical industry
- Education
- Emergency management

30 Government Accountability Office Report to Congressional Committees, *Homeland Security: Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State and Local Information Fusion Centers*, October 2007.

- Entertainment and retail
- Fire and emergency medical services
- Government
- Military
- Private security
- Postal and shipping
- Public health
- Telecommunications
- Transportation
- Utility and water.

These reports are exchanged between FCs and stakeholder agencies and are intended to educate the person(s) working for the agency who has a right and need to know. FCs often do not want these reports disseminated without their prior permission.

In addition to alerts, bulletins, and reports, FCs will provide assessments. These are usually for the locality under their jurisdiction. These assessments are used to generate the State of Affairs or an Annual Threat Assessment report that can be presented to the governor of the State and/or any other officials who have a need to know this information.

2.6 Communications Links

2.6.1 TMCs

TMC management often includes an approach to interagency cooperation—where the strategic missions of multiple stakeholders have overlapping elements. In these cases, open lines of communication are important for sharing information and coordinating in common mission areas. Common TMC communications linkages include:

- Face-to-face communications consist of personal interactions between staff from different agencies in co-located facilities such as joint operations centers or mobile command posts. When possible, it is effective for sharing information and coordinating response. Regular face-to-face interaction facilitates collaboration and trust.
- Radio is the most common form of communication between the field and operations centers to communicate on-scene traffic incident information. First responders such as law enforcement and safety/service patrols frequently use it. However, radio is often a challenging medium of communication between agencies because of the many different radio types and frequencies employed to maintain clear communications within each agency's own operating units.

- Wired telephones are the primary means of center-to-center interagency communication. They are still the most accurate and immediate method to describe transportation incidents. Hotlines can also establish a constant direct audio feed.
- Cellular telephones, which continue to improve technologically and gain in popularity, provide radio-like operability and wired-telephone connectivity and improve mobility. Push-to-talk systems and priority access mimic radio features.
- Alphanumeric pagers, cellular SMS text messaging, and email are used to communicate within and among agencies. Although still not a primary means of communication, advanced systems can include graphical maps, AVL, and in-vehicle mobile data terminals (MDTs) that can interact with CAD systems.
- CAD systems automatically dispatch services via a computer. A CAD system consists of a suite of software programs that can route calls, make dispatches, and monitor status. The program can send messages to responders via an MDT and can also be used to store and retrieve data. Responders in the field can receive messages via two-way radio, text message, pagers, and/or wireless telephone. Often, multiple agencies share systems to facilitate communication and increase efficiency.
- Video-imaging systems can be shared easily where partner agency staff members are co-located at TMCs. Video and still images can also be shared remotely via Internet portal. Video and images can also be shared with the media. Control of the pan-tilt-zoom functions on cameras can also be shared by agencies if desired. If such access is granted, protocols must be established on how and when such functions can be used.

Table 2-15 provides a summary of the TMC communication systems in terms of reliability, speed, security, and availability.

Table 2-15: TMC Communications Summary

Link System	Reliability	Speed	Security	Availability
Face-to-face	●	◑	●	◔
Radio	◑	●	○	●
Wired telephone	◕	●	◕	●
Cellular telephone	◑	◕	◑	◕
Pager/Text Messaging/Email	◑	◑	◑	◕
CAD	◑	◕	◑	◑
Video imaging	◑	◑	◑	◑
Key	●	= Good	○	= Poor

2.6.2 EOCs

The communications capabilities available to an EOC will generally depend on its primary jurisdiction. For example, a local community EOC's communications capabilities are likely to be more basic than those of EOCs serving a densely populated metropolitan area or a State. Table 2-16 presents the communications capabilities available and describes some of the characteristics associated with each.

Table 2-16: Available EOC Communications Capabilities

Capability	Characteristics
Wireline telecommunications	The wireline network (Public Switched Network) is ubiquitous. Although it is susceptible to physical damage (a backhoe operator may cut a fiber cable; a hurricane may uproot telephone poles; an accidental—or intentional—fire may destroy or damage key telecommunications facilities), telecommunications service providers have advanced technologies for rapidly rerouting communications traffic and have more than 100 years of experience restoring the physical infrastructure.
Wireless telecommunications	Although there are some areas where coverage may be limited or non-existent, the wireless network is rapidly becoming as ubiquitous as the wireline network. It offers greater mobility to users than the wireline network.
Two-way/high-frequency radio	The advantage of this communications capability is that it does not depend on the same communications infrastructure as the wireline and wireless networks and it offers mobility to emergency responders. However, it is often the case that the radio communications used by different emergency responders are not interoperable, even within the same jurisdiction (e.g., law enforcement officers may not be able to communicate with fire department personnel).
Commercial broadcast communications	Although these media offer only one-way communications, EOCs can use this communications capability to issue alerts to the general public and obtain information about developing incidents of interest.
Direct feeds	Some EOCs may have continuous, direct feeds from weather services and news organizations. This may provide information of interest more quickly than is the case with commercial broadcast communications.
Data links	Some EOCs may have data links to various information sources, which may give them access to sources of information not otherwise available and may also allow them to receive content in formats the other communications capabilities do not support (e.g., maps).
Human interaction	When ESF representatives are physically present in the EOC, and when emergency responders (e.g., police officers, firefighters, EMTs) are in the field, they exchange information (and have insights about that information and the situation) that make a substantial contribution to the coordination of the response effort.

2.6.3 FCs

Because of the investment, expertise, and capabilities that exist with FCs, the FC guidelines suggest that center plans support the jurisdiction's emergency management structure during crises. Since the State police primarily operate and control most FCs, the centers are involved in any natural disasters that may occur. Additionally, some FCs are beginning to co-locate with EOCs and have emergency management personnel working in their centers full time to help facilitate communications. FCs are expected to play a role during crisis management and recovery operations in coordination with the ICS, NIMS, and NRF.

Many FCs communicate via networks like HSIN. As an example of one of the main networks FCs use to communicate, HSIN gives FCs the ability to collaborate with other FCs and their Federal partner over an end-to-end encrypted network. HSIN provides communication, collaborative tools, and information.

U.S. Department of Homeland Security/Bahler

Thomas Muir briefs Secretary Napolitano about the flooding in North Dakota and Minnesota at the National Operations Center.

CHAPTER 3. OPPORTUNITIES FOR COLLABORATION

This chapter provides a description of information exchange possibilities to suggest opportunities for TMCs, EOCs, and FCs to explore and formalize processes and channels for collaboration—to the extent that the centers may find them beneficial.

This guidebook focuses mainly on the viability and practical use of TMC information resources by EOCs and FCs, but it also addresses opportunities for two-way information flows among all of the center types. The following sections outline transportation-related data managed and used by all three center types, and how center counterparts might use each kind of information. The sections are organized as follows:

- Transportation-related information managed and used by TMCs and how EOCs and FCs may utilize the information
- Transportation-related information managed and used by EOCs and how TMCs and FCs may utilize the information
- Transportation-related information managed and used by FCs and how TMCs and EOCs may utilize the information.

These sections distinguish among three basic categories of transportation-related information:

- Operational information (real-time or very recent)
- Records and logs information (recent or historical)
- Infrastructure information (locations, routes, dimensions, resources, nodes, etc.).

These categories of information have strong value implications for each center type, depending on the mission, jurisdictional, and temporal focus of each center.

Each type of center—TMC, EOC, and FC—operates under different (and in some cases overlapping) missions. Their missions determine the categories of transportation-related information that they collect and use, as well as the official sources and information that may be beneficial if available from other types of centers. In fact, the three center types already often obtain and process similar information from external sources. Examples are news feeds, weather information, and 911 call/dispatch data.

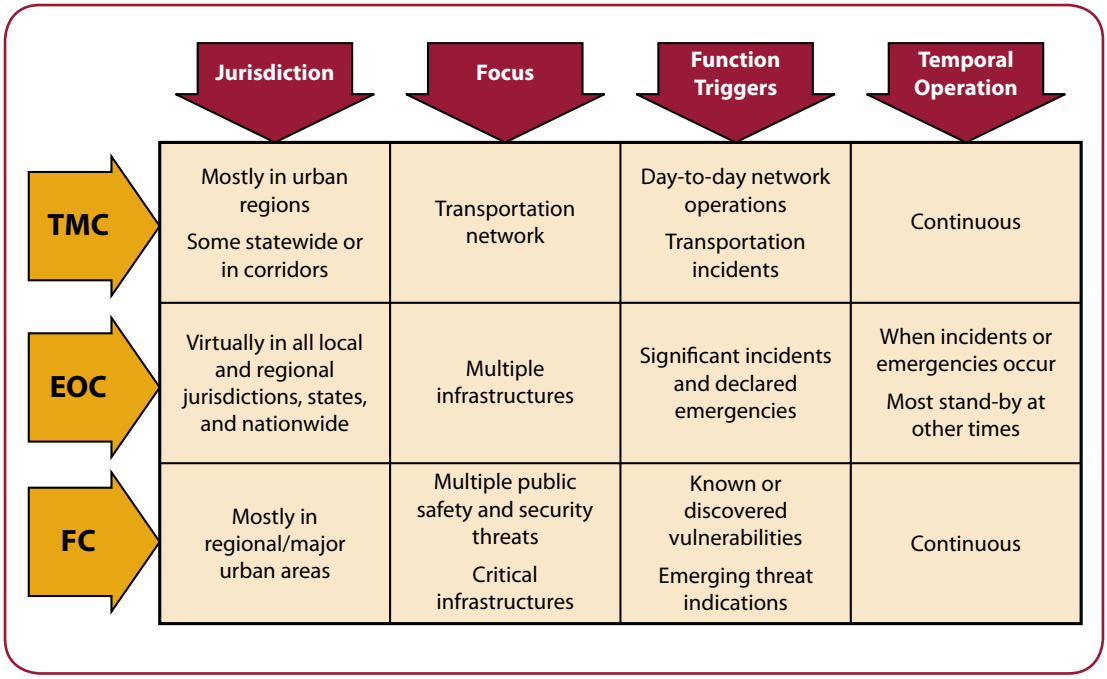
Figure 3-1 illustrates the differences in typical characteristics of the center types with respect to the overall focus of their respective missions. Each characteristic should be seen as a continuum.

The characteristics used to typify centers include:

- Geographical coverage (i.e., does the center focus primarily on the local, regional, statewide, national, or global environment?)
- Infrastructure focus (i.e., does the center focus on one particular infrastructure, such as the transportation infrastructure, or does it focus on multiple infrastructures?)
- Temporal nature of mission or operations (i.e., does the center focus primarily on today's situations, or does it focus on situations that may occur in the future?)
- Functional roles (i.e., does the center focus on operational functions or on analytical functions?)
- Deployment triggers (i.e., does the center focus primarily on reacting to adverse situations or on preventing them?).

There are, of course, wide variations in the characteristics of specific TMCs, EOCs, and FCs. For example, EOCs (in some form) exist at virtually every jurisdictional level. But the context of this guidebook involves regular regional and local information-sharing relationships between proximate or linked centers of the three types.

Figure 3-1: Comparison of Typical TMC-EOC-FC Characteristics



The following sections describe transportation-related information that is managed and used by each type of center and how it could be leveraged effectively by other types of centers.

3.1 Transportation-Related Information Managed/Used by TMCs

The primary mission of a typical TMC is to monitor traffic and facilitate efficient movement on regional transportation infrastructure. To meet these goals, TMCs employ a variety of technologies to gather and use information related to the status and operations of the local or regional transportation infrastructure, including highways, bridges, arterials, and transit operations. TMCs can share information gathered about the infrastructure with other local agencies that need to gain insight as to the status of any or the entire infrastructure, including EOCs and FCs. TMCs are responsible for a variety of categories of information related to the management of their transportation infrastructures.

3.1.1 Information Categories

TMCs manage and use all three of the primary categories of information:

- Operational information, including real-time situational traffic and network status information gathered by ITS resources, sensors and surveillance equipment, safety/service patrols, vehicles equipped with IntelliDrive[SM] OBE, and other internal or external sources.
- Records and logs of special events, incidents, and emergencies affecting, either directly or indirectly, the transportation infrastructure. TMCs also typically record network statistics and traffic data.
- Infrastructure information including maps, resources, and physical data on transportation infrastructure assets and operating condition.

Table 3-1 summarizes operational information and its potential use to other center types. Details and considerations are summarized in the text following Table 3-1.

Table 3-1: TMC *Operational Information*: Description and Potential Uses by EOCs and FCs

TMC Information	Potential Uses	
	EOCs	FCs
Transportation and ITS infrastructure disruptions (e.g., disruptions due to power outages, flooding, communications breakdown)	• Determine how disruptions will affect response team activities • Support continuous situational awareness during an incident	• Determine how disruptions may result in cascading effects on CIKR
IntelliDrive[SM] probe data and algorithm results	• Continually update evacuation routes • Re-route first responders	• Develop advanced algorithms for early warning of secondary incidents • Develop advanced algorithms for threat assessment

TMC Information	Potential Uses	
	EOCs	FCs
Incidents that potentially impact transportation operations (e.g., industrial accidents, civil disruption, hostage situations)	• Determine whether incident warrants alerts or notification to the public and responders	• Use information for threat assessment
Traffic incidents	• Determine how disruptions will affect response team activities	• Traffic incidents may be monitored to identify patterns and potential for secondary incidents
Video camera feeds	• Visually confirm situational information from other sources • Assist with an emergency evacuation	• Maintain situational awareness and factor information into incident response measures[31]
Planned projects that impact the transportation infrastructure (e.g., surface and subsurface construction and maintenance)	• Assist informed planning of emergency response activities	• May use this information in conjunction with other data to assess threats
Special events in progress that potentially impact transportation operations (e.g., sports event)	• Determine whether the special event warrants alerts or notification to the public and responders	• Use information for threat assessment depending on the special event
Planned special events and associated road closure/traffic pattern data	• Plan for potential emergencies • Support continuous situational awareness	• Information[32] used to determine impact on other activities (e.g., visit of high-profile person)
Activity/inactivity and operational status of: • *Bridges* • *Tunnels* • *HOV/HOT lanes* • *Reverse lanes* • *Weigh stations*	• During an incident, monitor status of conditions and inform affected stakeholders (nature and extent of the incident will determine the level of coordination and participation)	• Information used to determine impact on other activities (e.g., tunnel closure requiring HazMat rerouting)

31 Some FCs are co-located with EOCs or have access to video feeds. Those FCs that do not have such access can use the TMC Web site or other open source Web sites to monitor traffic cameras in the area.

32 Information is used when planning for special movements of people or materials. Information can be exchanged as movements are taking place for situational awareness of law enforcement personnel.

TMC Information	Potential Uses	
	EOCs	FCs
Localized surface and atmospheric conditions (e.g., icing, fog, water table level status)	• Determine how road surface conditions will affect response team activities • Support continuous situational awareness during weather events	• Possible notifications to stakeholders for safety/ preparation for ongoing operations •
Emergency management notification status (e.g., roadway HazMat incident)	• Use information to determine activation levels	• Use information to coordinate resources as needed • Monitor situation and report updates as needed to stakeholders, both internal and external, depending on the situation
Localized traffic flow data (e.g., speed)[33]	• Determine impact on emergency responders • Evaluate alternate routes	• Monitor traffic during planned special events
DMS status (including location, direction, message)[34]	• ***Everyday incidents:*** EOC defers to TMC and responders on everyday incidents • ***Emergencies:*** EOC will coordinate messages and incidents requiring multi-agency collaboration	• Useful for posting messages such as Amber and Silver Alerts
Status of: • *Transit operations and ridership* • *Public parking capacity* • *Bridge posting*	• Incident deployment and evacuation management	• Location of bus and rail vehicles relative to security sensitive buildings

3.1.1.1 Transportation and ITS Infrastructure Disruptions

Description: TMCs use a variety of resources, including ITS and personnel, to track the current condition of transportation and ITS infrastructure and potential disruptions, including disruptions due to power outages, flooding, and communications breakdowns. When operable, video feeds provide an excellent opportunity for TMCs to assess the situation on the transportation network. This information can be shared with EOCs and FCs via a Web portal. In many TMCs, cameras contain power and communications redundancies to allow continued use in case of a disruption. However, in a severe communications breakdown, even redundant systems can collapse.

33 Accessed via police, TMC, or mobile video systems (forward command systems). Open sources can be accessed as well but do not provide the control of the camera that may be needed in certain incidents.

34 Most of this information is monitored by State police (HOV violations, ramp metering).

Potential Uses by EOCs: If such disruptions had a significant impact on an EOC's jurisdiction (e.g., a collapse of a bridge carrying hundreds of vehicles during rush hour in a large metropolitan area) and the EOC was in the monitoring phase, this information may be used to determine whether to go into the activation phase. In most circumstances, however, where a disruption is less severe, an EOC may use this information only when it has already been activated and when the information would be useful as part of continuous situational awareness and to determine how such a disruption may affect response team activities. For example, disruption to a key arterial may require re-routing response teams or changing evacuation plans.

Potential Uses by FCs: Information concerning transportation and ITS infrastructure disruptions could be used by an FC to determine how disruptions may produce cascading effects for critical infrastructure assets.

3.1.1.2 Incidents that Potentially Impact Transportation Operations

Description: TMCs monitor non-transportation incidents that could indirectly impact transportation operations including industrial accidents and chemical spills, civil disruption, and hostage situations. While not directly related to transportation movements, TMCs must be aware of any incidents that could potentially affect transportation operations and respond accordingly, potentially coordinating operations with other agencies. For example, while a major chemical spill at a regional port would not directly affect highway or arterial infrastructure, it might require an evacuation of all people within a certain radius of the spill. The TMC would be required to work to ensure that necessary steps toward a full evacuation are taking place.

Potential Uses by EOCs: As with disruptions to the transportation infrastructure itself, this type of incident may also endanger the public or impede emergency responders. Because both types of situations have the same impact on emergency response, EOCs would use information on these incidents both to determine whether to activate (if the incident profoundly affected the EOC's jurisdiction) or to determine how a given incident may affect response team activities.

Potential Uses by FCs: Information about incidents that could potentially impact overall transportation operations can aid an FC's overall coordination effort during an emergency, depending on the incident. However, State police usually manage the day-to-day operations and are on alert for these activities (HOV violations, ramp metering issues). The FCs also often monitor radio communications concerning potential incidents.

3.1.1.3 Traffic Incidents

Description: TMCs track traffic incidents that occur on highways and arterials, often taking proactive steps to remove the incident to prevent additional congestion and crashes, and maximize road capacity. Using ITS resources such as CCTV cameras, TMCs identify and verify traffic incidents. Safety/service patrols can also identify and verify incidents, relaying situational information to the TMC. Once a safety/service patrol operator, State police, or other responder verifies an incident, the TMC directs actions to remove the incident from the roadway through a coordinated traffic incident management (TIM) response. In many TMCs,

traffic incidents are recorded and displayed on the Web in real time to inform TMC stakeholders and roadway users. Incidents may also be reported to drivers via 511 systems.

***Potential Uses by EOCs*:** During the monitoring phase, information on traffic incidents would not usually be of interest to the EOCs. During the activation phase, EOCs would find this information useful in determining how such disruptions will affect response team activities.

***Potential Uses by FCs*:** FCs may monitor traffic incidents to help identify patterns and analyze the potential for secondary incidents. For high-profile traffic incidents or major crashes, FCs are often notified by the State police dispatch so that the FC has an awareness of what is going on in case another incident occurs before the initial incident is resolved.

3.1.1.4 Video Camera Feeds

Description: Most TMCs own and operate CCTV cameras focused on the roadway infrastructure. The TMCs use these cameras to obtain situational awareness of the transportation infrastructure, which can be shared with partner agencies through a direct Web portal as well as to both agencies and system users through the Web site, www.trafficland.com. TMCs connect to cameras via T1 lines, often with back-up dial-up connections. Additionally, some TMCs have the capability to record and retain traffic data for a period of hours or days. Others do not possess any recording capabilities generally due to privacy and litigation concerns.

***Potential Uses by EOCs*:** In most situations, EOCs would not find this information useful. However, in the activation phase, information from video camera feeds may be used to confirm situational information from other sources. Because initial reports may be inaccurate, or an initial report from one source may conflict with that from another, the video camera feeds can help the EOCs achieve a more accurate understanding of a situation. For example, live video could be very useful in monitoring traffic conditions during an evacuation. As part of the *i*Florida project, Florida's statewide EOC (SEOC) was connected to the Florida DOT's (FDOT's) 25 Statewide monitoring cameras. To provide improved access to the video feeds, the SEOC upgraded the bandwidth of its network connection with FDOT's system. Prior to this connection, the SEOC could get access from FDOT's traffic monitoring locations, but it was not real-time data and was provided as part of a public web site that the SEOC could monitor. The iFlorida project final report includes additional information about the use of ITS to support hurricane evacuations.[35]

***Potential Uses by FCs*:** Since some FCs are co-located with EOCs, they will have access to video feeds as long as an EOC is tied into a video network. For traffic-related issues, those FCs that do not, or cannot, utilize EOC or TMC video feeds will access traffic cameras via public or private sector Web sites that have access to traffic cameras in the area. However, access to Web-based video cameras does not offer the control, or access to the controllers, that an FC might need to pan and zoom. FCs can use the information provided by video cameras to maintain situational awareness and will factor information provided by the cam-

35 U.S. Department of Transportation, Federal Highway Administration, i*Florida Model Deployment Final Evaluation Report*, 2009, http://ops.fhwa.dot.gov/publications/fhwahop08050/chap_9.htm, accessed 2010.

eras to determine incident response measures. If the cameras also cover critical infrastructure, FCs could monitor such infrastructure as required. Such cameras may be in addition to those surveillance cameras sometimes deployed by law enforcement agencies that are generally not available to TMCs for monitoring traffic. In some locations, such as the City of Chicago, law enforcement personnel can monitor surveillance cameras installed in the "Loop" area (i.e., the historic city center) for law enforcement purposes. These cameras can also provide secondary traffic incident information. Shared use of images from both TMC and FC cameras may be a topic for further exploration by these organizations.

3.1.1.5 Planned Projects That Impact the Transportation Infrastructure

Description: TMCs maintain awareness of planned projects and construction that affect transportation operations, both directly and indirectly. This could include both surface and subsurface construction and maintenance for transportation infrastructure, utilities, and other construction projects such as new buildings. If a planned construction project will disrupt traffic flow, TMCs take active steps to create detours and other mitigation strategies.

***Potential Uses by EOCs*:** EOCs could use this information to build their emergency response plans. For example, if a portion of an interstate highway within the EOC's jurisdiction was under construction, advance notice of this activity would allow an EOC to evaluate alternate routes and adapt its response plan accordingly until completion of the construction. This would be particularly important when reviewing evacuation plans in preparation for hurricane season, for example.

***Potential Uses by FCs*:** Normally, an FC will receive notifications about major road closures in advance for two reasons:

- To coordinate State police efforts to have a patrol car and officer in place to protect workers during construction
- To maintain a list of major/long-term road closures in case of an evacuation and/or be able to identify any false closing of roads by a criminal entity near a section of critical infrastructure (e.g., bridge).

Information about planned projects that will impact the transportation infrastructure can be used in conjunction with other data to assess threats.

3.1.1.6 Special Events in Progress That Potentially Impact Transportation Operations

Description: In addition to planning for projects and construction that affect transportation infrastructure, TMCs track and monitor special events in progress that have the potential to impact transportation operations including sports events, concerts, and parades. Some special events will have a known effect on transportation operations, including regularly scheduled special events. However, other events that do not take place on a regular basis, like a victory parade for a sports team, may have far-reaching consequences that are unknown. Additionally, mismanagement or unforeseen circumstances of a planned special event can lead to an incident.

***Potential Uses by EOCs*:** EOCs could use such information while in the monitoring stage to contribute to situational awareness so they could consider the event should an incident occur that warrants advancing to the activation stage.

***Potential Uses by FCs*:** FCs will use information about special events in progress that potentially impact the transportation infrastructure operations as part of their role in the coordination effort during the event. Information about special events in progress will be reported to the FCs depending on the incident (e.g., natural disaster, shooting, hostage situation requiring road closures, operational support/tactical team deployment). FCs will then work to coordinate this information with their partner organizations and agencies.

3.1.1.7 Planned Special Events and Associated Road Closure/Traffic Pattern Data

Description: TMCs are part of the planning process for planned special events including developing congestion mitigation strategies for potential transportation bottlenecks.

***Potential Uses by EOCs*:** Depending on the duration and the extent of the impact on the transportation infrastructure, this information may be useful to EOCs in their planning activities. For example, a special event such as the Olympics would have significant impact on evacuation plans, and the EOCs would need to adapt such plans in case an incident occurred that warranted evacuation. Some special events may require pre-positioning of medical and law enforcement personnel and firefighters. This information is also useful because it supports continuous situational awareness.

***Potential Uses by FCs*:** Planned special events and the road closures/traffic pattern data associated with them are used to determine impact on other activities. This information is used when an FC is engaged in planning for special movements of people (e.g., visit of high-profile person, convoy operations of VIPs/high-profile prisoners) or materials. An FC could be on the lookout for demonstrations, explosions, shootings, etc. on major roads that, combined with planned special event data, could impact their operations. Data is exchanged in real time, and the FCs disseminate the information to give the agencies involved, usually law enforcement, a better level of situational awareness. Information about planned special events and associated road closure/traffic pattern data is used on an as-needed basis.

3.1.1.8 Activity/Inactivity and Operational Status of Critical Infrastructure

Description: TMCs track the operational status of critical transportation infrastructure. In addition to knowing whether a piece of infrastructure is active or inactive, TMCs can track aspects of the infrastructure including number of lanes in use and approximate average traffic volume and speed. Some of the types of critical infrastructure that TMCs typically track include:

- Bridges
- Tunnels
- HOV/HOT lanes
- Reverse lanes

- Commercial vehicle weigh stations.

***Potential Uses by EOCs*:** During the monitoring stage, this information may not be useful for EOCs because such operational status is in continuous flux. However, during the activation stage, EOCs could monitor the status of conditions and inform affected stakeholders and the public if required. The nature and extent of the incident that resulted in activation will determine the level of coordination and participation required.

***Potential Uses by FCs*:** The operational status of transportation assets can be information that an FC uses to determine the impact on other activities (e.g., tunnel closure requiring HazMat rerouting).

3.1.1.9 Localized Surface and Atmospheric Conditions

Description: Road Weather Information Systems (RWIS), a series of small sensors embedded in the transportation infrastructure, provide the TMC with information regarding localized surface and atmospheric conditions. TMCs have the ability to detect the temperature of both the local atmosphere as well as the pavement surface. Additionally, moisture sensors have the ability to detect the presence of moisture on the pavement. In combination with other ITS sensors such as CCTV, TMCs can detect such weather events as icing, fog, and water-level status.

***Potential Uses by EOCs*:** As with the operational status of transportation infrastructure components such as bridges, tunnels, HOV/HOT lanes, reverse lanes, and weigh stations, localized surface and atmospheric conditions are continually in flux and would not have great utility for an EOC during the monitoring stage. However, once an EOC is activated, this information becomes useful in anticipating how road surface conditions might affect response team activities and in supporting continuous situational awareness during emergency response.

***Potential Uses by FCs*:** While information on localized surface and atmospheric conditions will be available via multiple sources, FCs can pass along notifications to partner agencies and/or Regional Intelligence Centers (RICs) to help them safely plan for operational activities or to make adjustments to existing/ongoing operations. If an incident response is warranted due to a severe weather event, FCs will send out notifications to stand up coordination activities. FCs will coordinate their efforts with the EOCs to provide emergency response support to such incidents as road closures and traffic management issues caused by localized surface and atmospheric conditions. These resources could include State and local police assets depending on the FC.

3.1.1.10 Emergency Management Notification Status

Description: TMCs flag incidents and emergencies on transportation infrastructure and can alert partner agencies and other stakeholders of such occurrences. Using ITS assets, TMCs have the ability to detect some emergencies before other responders. For example, a TMC might have knowledge of the location of a HazMat spill on a major interstate and may be able to provide early information about the hazardous material that was spilled so responders can arrive at the scene properly equipped.

***Potential Uses by EOCs*:** EOCs may use this information to determine whether EOC activation is warranted.

***Potential Uses by FCs*:** FCs use emergency management notification information to coordinate resources, as needed, during an incident, emergency, or natural disaster. FCs will monitor the situation and report updates to partner agencies, both internal and external, depending on the type of situation.

3.1.1.11 Localized Traffic Flow Data

Description: Using ITS resources including CCTV and loop detectors, TMCs have situational information related to the movement of traffic including current traffic speed and volume. This data can be disseminated to the public and other agencies via a Web portal with a real-time map indicating average traffic speed and reported through a 511 system. As well as being a key indicator for traffic incidents and other traffic bottlenecks, TMCs can utilize flow data for roadway capacity and congestion planning.

***Potential Uses by EOCs*:** This information is also in continuous flux, so it would only be useful to EOCs when they are activated and they may use it to determine the impact on emergency responders.

***Potential Uses by FCs*:** If FCs are monitoring a special event, such as a visit by a high-ranking official or a National Special Security Event (NSSE),[36] information about current traffic conditions could be helpful in monitoring and/or adjusting motorcade operations or other transportation needs surrounding an NSEE.

3.1.1.12 DMS Status

Description: DMS are programmable electronic signs displayed along roadways as both permanent fixtures and movable displays. The signs can be programmed for the TMC to display traffic, weather, congestion, alternate route, or emergency information to system users. It is important for motorists to be able to comprehend the information posted on the DMS so FHWA has published the *Changeable Message Sign Operation and Messaging Handbook* to provide guidance on day-to-day messages as well as emergency messages.[37] TMCs generally communicate with signs via a T1 Internet connection. Often, a dial-up connection serves as a back-up system. If the connection between the TMC and the sign is severed, but power to the sign remains, the sign usually continues to display its most recent message. Using their connection with the sign and receiving verification via CCTV cameras, TMCs have information regarding the location (including which direction of traffic the sign faces) and the current message being displayed.

***Potential Uses by EOCs*:** During routine incidents (e.g., a car crash that may impede or block traffic until it has been cleared), EOCs would defer to the TMC and responders. However,

36 According to DHS, a number of factors are considered when designating an event as an NSSE including: 1) anticipated attendance by dignitaries, 2) size of the event, and 3) significance of the event.

37 U.S. Department of Transportation, Federal Highway Administration, *Changeable Message Sign Operation and Messaging Handbook*, 2004, http://tmcpfs.ops.fhwa.dot.gov/cfprojects/uploaded_files/CMS%20Operation%20and%20Messaging%20Handbook-Final%20Draft.pdf, , accessed 2010.

during emergencies, EOCs may coordinate messages and incidents for posting on the DMS that require multi-agency collaboration. One example may be during an evacuation prior to a hurricane, in which the EOCs may collaborate with the TMCs regarding the messages displayed to direct citizens to the evacuation routes and shelters.

Potential Uses by FCs: The primary use for DMS is to post traffic conditions and incident information for motorists. However, they have also been used for specialized law enforcement purposes such as the posting of Silver Alerts and AMBER Alerts. The AMBER Alert™ Program is a voluntary partnership among law enforcement agencies, broadcasters, transportation agencies, and the wireless industry, to activate an urgent bulletin in the most serious child-abduction cases. The program has specific criteria under which an AMBER Alert will be posted on a DMS. Understanding the status of the DMS will allow law enforcement agencies and TMCs to cooperate in more quickly posting any necessary information. See http://www.amberalert.gov/ for additional information on the program.

3.1.1.13 Status of Transit Operations and Ridership, Public Parking Capacity, Bridge Posting

Description: TMCs located in areas with transit operations generally have some level of integration with local transit operations. Transit-focused TMCs monitor and control transit bus and rail fleets to maximize coordination and efficiency. Transit vehicles can also be guided and utilized in emergency situations such as evacuations.

Some TMCs have the capability to monitor parking capacity. Parking areas can be utilized in emergency situations for a mobile operations center or to stage responder vehicles.

TMCs track regional bridge postings. Bridge postings can include height/weight restrictions, HazMat restrictions, weather warnings, etc. These postings help the TMC determine the current proper use of bridges.

Potential Uses by EOCs: This information is potentially relevant to incident deployment and evacuation management.

Potential Uses by FCs: Information on the location of bus and rail vehicles relative to the locations of security-sensitive government buildings might be useful to FCs both in monitoring day-to-day operations and in incident response.

Table 3-2 summarizes records and logged information and its potential use to other center types. Details and considerations are summarized in the text following Table 3-2.

Table 3-2: TMC Records and Logs Information: Description and Potential Uses by EOCs and FCs

TMC Information	Potential Uses	
	EOCs	FCs
Incident Logs	• Determine need for emergency responders • Support performance measurement for incident response planning purposes	• Traffic incidents may be monitored to identify patterns and potential for secondary incidents
Historical network statistical records • *Typical traffic pattern data* • *Toll transaction records* • *Red-light and speed camera records* • *Traffic records* • *Weather records* • *Recorded – retained video data*	• Information could be used to support planning for detours and/or an evacuation • Information could be used to support exercise scenario development	• Statistical support for annual risk assessments[38] • Potential law enforcement applications

3.1.1.14 Incident Logs

Description: TMCs track reported traffic incidents on the roadway system for which they are responsible and may have the capability to monitor/record incidents on other roadway systems. Traffic incidents are sometimes reported by a responder, such as a safety/service patrol operator and State police, and recorded by the TMC and/or CAD system. Information includes date, time, location, responder(s), and a detailed description of the incident. Often, incident logs are available in real time via the Internet. The time of day when the incident is cleared is often recorded to assist in performance measurement.

Potential Uses by EOCs: These logs may assist in after-action reporting and revisions to SOPs as well as workforce planning for incident response. Many agencies measure response times to evaluate the effectiveness of their TIM programs and how well they are coordinated with other emergency responders to reduce response times and clear roadway incidents as quickly as possible to avoid congestion and the possibility of secondary incidents.

Potential Uses by FCs: An FC will monitor traffic incidents to identify whether there are patterns and potential for secondary incidents. Incident logs are not kept at FCs according to one source, but they will have access to this information on an as-needed basis via State Police Division Offices and/or the TMC operator.

3.1.1.15 Historical Network Statistical Records

Description: TMCs track statistical measures of local traffic conditions including:

38 State police divisions will provide to FCs if requested.

- Typical traffic pattern data including daily congestion patterns
- Toll transaction records
- Red-light and speed camera records
- Traffic records
- Weather records
- Recorded – retained video data.

Potential Uses by EOCs: EOCs have a role in evacuation planning, and information such as historical traffic data, congestion patterns, and speed data can be useful in planning evacuation operations. Likewise, EOCs are often responsible for developing training and exercises, and the historical data could be used to assist in scenario development for such exercises.

Potential Uses by FCs: Historical network statistical records will support an FC as it develops its annual risk assessments. These records are not kept at the FCs, but FCs will have access to this information via State Police Division Offices and/or the TMC operator. Recorded video images from CCTV can sometimes be considered for use in law enforcement operations. If such a use is contemplated, strict controls on the images captured and stored must be defined and followed to ensure the information can be used in legal proceedings.

Table 3-3 summarizes physical infrastructure information and its potential use to other center types. Details and considerations are summarized in the text following Table 3-3.

Table 3-3: TMC Physical Infrastructure Information: Description and Potential Uses by EOCs and FCs

TMC Information	Potential Uses	
	EOCs	FCs
Maps/GIS[39]	• Develop training, testing, and exercise programs • During incidents to give a better operating picture to response teams and coordinating agencies (e.g., fire stations)	• Infrastructure information awareness and planning, vehicle tracking, and incident response support
Critical infrastructure locations	• Prioritize response efforts	• Assess the impact of critical infrastructure failure (e.g., overall impact that damage to a particular train bridge would have on a city)

39 Critical information is stored in databases to be accessed depending on the nature of the incident and provides readily available data for rapid response to incidents (e.g., shelters, schools, pharmacies). Information may include graphic information on metro station incidents and closures; evacuation routes; medical evacuation activities; decontamination sites; and proximity to schools, hospitals, and HazMat or industrial sites.

TMC Information	Potential Uses	
	EOCs	FCs
Population/building density maps[40]	• Prioritize response efforts and assess response resources required	Planning and modeling purposes such as: • To help first responders conduct damage assessments following incidents • As input for risk assessments (e.g., determining the value of a particular target)
Shelter locations[41]	• Direct people to safe areas and assess deployment of supplies and support personnel (e.g., American Red Cross, medical personnel)	• Planning and modeling purposes
Transportation infrastructure statistics (e.g., locations and number of bridges, number of overpasses, posting status)	• Use a ready reference display of critical infrastructure information stored in databases to be accessed depending on the incident including bridge, overpass, and/or tunnel status (e.g., active/closed/posted). Specific information pertaining to weight, wind resistance, load, etc., will require professional individual insight and will not always be stored in data files by the EOC • Used to coordinate with other internal and external agencies	• Critical infrastructure assessments • Locations are monitored during incidents to identify a trend or an evolving terrorist incident[42]
HazMat routing information	• Response team planning activities and/or general awareness	• Monitor information for planning purposes and during a high-profile incident. Routes will be monitored and evaluated for vulnerabilities

40 May be included in GIS information.

41 May be included in GIS information.

42 Information typically kept by the FC analyst/specialist for a particular infrastructure.

TMC Information	Potential Uses	
	EOCs	FCs
System configuration (e.g., bridge clearance, access, type)	• Deploying responders and equipment[43]	• Use for statistical support for annual risk assessments. Information on pavement thickness and connection points to the main roads on the system is used for vulnerability assessments
Parking, station, and terminal locations	• Manage an evacuation	• Vulnerability assessments
Sensor and camera locations	• Use for situational awareness	• Plan for monitoring • Surveillance of critical infrastructure
Locations and types of traffic control devices	• Coordinated traffic control at incident locations • Emergency responder routing	• Route planning and special events management

3.1.1.16 Maps/GIS

Description: Many TMCs have the capability of GIS automatic mapping. Such programs can continuously update mapping features and locations of ITS devices for incident management. GIS applications are capable of locating a street, intersection, or other feature based on vector data. Programs can also display raster images (bitmaps), aerial photos, or street directory maps.

Potential Uses by EOCs: It is very important to have reliable and readily available mapping and location information for display and assessment of the extent of an incident's effects and for clear communication of tactics as resources are deployed. In a large-scale response when responders may be from outside the immediate area, readily available maps are essential for their use.

Potential Uses by FCs: Most FCs use ArcGIS or similar software products. They use these mapping products to provide them with information on:

- Infrastructure
- Tracking of vehicles
- Support for incident response activities including:
  - Tracking road closures
  - Evaluating and monitoring evacuation routes
  - Determining medical evacuation areas and decontamination sites
  - Learning the proximity of schools, hospitals, and HazMat/industrial sites to an incident.

43 Information pertaining to weight, wind resistance, load, etc., will require professional individual reference and will not always be stored in data files by the EOC.

Mapping and GIS are also used for infrastructure information awareness, exercises, and planning purposes.

3.1.1.17 Critical Infrastructure Locations

Description: TMCs are aware of the locations of identified critical infrastructure including critical buildings, major roadways, evacuation routes, bridges, and tunnels.

***Potential Uses by EOCs*:** This information assists in situational assessment and rapid judgment of risks to critical infrastructure for emergencies in which physical proximity is a critical risk.

***Potential Uses by FCs*:** FCs use critical infrastructure information to assess the impact of infrastructure failure or vulnerability to attacks. For example, an FC may use this information to determine the overall impact that damage to a particular bridge would have on a city. This information is normally held by an FC analyst/specialist for that particular infrastructure. An analyst tasked with rail infrastructure will have information on all the bridges the train transits, the volume and type of explosives needed to bring the bridge down, bridge placement, and weak-points, etc. The analyst/specialist will also analyze the debilitating effect of one piece of infrastructure being disabled versus another (e.g., in Washington, DC, what effect does the Key Bridge being out of service have versus the Memorial Bridge being out of service?).

3.1.1.18 Population/Building Density Maps

Description: Using GIS and other data resources, TMCs can map local populations including locations and densities. For example, the locations of specific populations that might require transportation assistance in an evacuation could be mapped along with their proximity to public transportation.

***Potential Uses by EOCs*:** This information assists in situational assessment and rapid judgment of risks to the public and commerce for emergencies in which physical proximity is a critical risk.

***Potential Uses by FCs*:** FCs use population and building density maps, much like mapping and GIS, for planning and modeling purposes. The centers use this information to aid first responders in their efforts as well as to conduct damage assessments following incidents. For risk assessment purposes, population and building density maps provide input for determining the value of a particular target.

3.1.1.19 Shelter Locations

Description: In case of an evacuation, TMCs know the locations for designed shelters, shelter capacities and amenities, and potential highway routes leading to and away from shelters. They also have an inventory of traffic monitoring and control devices in the vicinity of shelters. One example is DMS that could provide shelter location information to motorists.

***Potential Uses by EOCs*:** When reliable, and when connected to current mapping data, information enables coordination and effective control of routes and dispatching of evacuation operations.

***Potential Uses by FCs*:** FCs may use this information for planning and modeling purposes. This information can be stored in mapping and GIS databases and referred to during incidents and emergencies to aid first responders and assess a possible threat. In addition, law enforcement agencies are often tasked with providing security at shelter locations, so readily available shelter location information could aid in deploying these law enforcement resources.

3.1.1.20 Transportation Infrastructure Statistics

Description: TMCs have detailed statistics on the number and location of bridges and overpasses. Additionally, they are aware of relevant postings on infrastructure including the height/weight restrictions on bridges and HazMat restrictions in tunnels.

***Potential Uses by EOCs*:** These statistics support operational decisions involving the movement of heavy equipment and buses, as well as determination of physical risk to transportation infrastructure during emergencies.

***Potential Uses by FCs*:** Critical transportation infrastructure locations are monitored during an incident to identify a trend or an evolving terrorist incident. The FC analyst/specialist who is tasked with that particular infrastructure typically keeps this information. FCs can also use transportation infrastructure statistics information for annual infrastructure assessments.

3.1.1.21 HazMat Routing Information

Description: In addition to recommended HazMat routes, TMCs also keep information regarding bridge and tunnel postings that might place restrictions on various types of hazardous materials moved via highway and/or rail facilities.

***Potential Uses by EOCs*:** This information may aid planning for potential HazMat-related emergencies, risk assessment during emergencies, and routing of the removal of dangerous materials. HazMat may also need to be re-routed in case an incident impacts its primary route.

***Potential Uses by FCs*:** FCs will monitor information on HazMat movements when information is made available to them. They will be involved in the planning process for a high-profile movement or during a HazMat incident. The FC will monitor the routes that HazMat will take and will evaluate them for vulnerabilities prior to the movement. An FC is an active participant during a high-profile incident by sharing and coordinating information to ensure safe passage of the material.

3.1.1.22 System Configuration

Description: TMCs have records on infrastructure configurations including the bridge and tunnel type, access limits, clearances, and weight restrictions.

***Potential Uses by EOCs*:** Information could be useful for assessment of risk to infrastructure and/or alternative response tactics involving use of the transportation network. For example, if specialized equipment that is overheight and/or overweight is required for a

response, access to such system information will allow for quicker designation of safe highway access routes.

***Potential Uses by FCs*:** The FC can use system configuration information for statistical support of its annual risk assessments. Any information on thicknesses or connection points of pieces of critical infrastructure along major arterials is used as part of the vulnerability assessments.

3.1.1.23 Parking, Station, and Terminal Locations

Description: TMCs have records on parking facilities, capacity limits, and potentially even current capacity. Additionally, TMCs that focus on transit operations have plans of transit, vehicles, stations and terminals, and system ridership and capacity.

***Potential Uses by EOCs*:** This information is useful to EOCs for managing clearance of vehicles and people from incident locations, or for managing staging tactics for response teams.

***Potential Uses by FCs*:** In conducting vulnerability assessments, FCs should consider parking areas serving large numbers of people such as transit stations and terminals. Information about the number of parking spaces, layout of the parking area, whether the parking is an at-grade or multi-level facility, and other such information can be useful in assessing the vulnerability of such locations.

3.1.1.24 Sensor and Camera Locations

Description: TMCs have records of locations of all traffic sensors and CCTV cameras including the direction in which the asset is focused and the approximate camera angle.

***Potential Uses by EOCs*:** This information may aid in determining whether visual or sensor information is available for specific incident sites to direct camera resources quickly and accurately.

***Potential Uses by FCs*:** FCs can use the locations of sensors and cameras to develop a plan for monitoring critical infrastructure and/or routine traffic conditions. As an example, some bridges in central Florida are equipped with a sensor that will sound an alarm at the TMC if a truck or other large vehicle is parked underneath the bridge for a certain time period. The cameras could then be used to evaluate that vehicle to determine whether law enforcement action is necessary.

3.1.1.25 Locations and Types of Traffic Control Devices

Description: TMCs have records on locations of traffic control devices including emergency vehicle preemption signal control, variable speed limit devices, HOV facilities, reversible flow lanes, and ramp metering and closures.

***Potential Uses by EOCs*:** This information could be useful to EOCs for coordinated traffic control/diversion tactics in the vicinity of incidents. It may also be useful for routing emergency responders particularly through traffic signals with emergency vehicle signal preemption.

Potential Uses by FCs: This information could be useful to FCs for route planning for dignitaries requiring a secured roadway route and/or planning and management of special events.

3.1.2 Summary of Transportation-Related Information Managed/Used by TMCs

TMCs own and manage a variety of information related to the management of transportation infrastructure, including both current and historical data. As part of their mission focus, EOCs and FCs are also responsible for the safety of transportation operations, although not necessarily on a daily basis.

- EOCs must maintain specific knowledge of real-time transportation operations and detailed understanding of existing transportation infrastructure to plan for and conduct emergency operations for their jurisdiction. Furthermore, some special events and incidents, and emergencies involving the transportation infrastructure, require EOC participation.
- FCs are responsible for gathering information for a variety of external sources, consolidating the data, and making judgments regarding hazard operations, potential threats, and criminal prosecution. As part of this mission, transportation-related information plays an important role in the information they receive and analyze.

3.2 Transportation-Relevant Information Managed/Used by EOCs

The primary EOC mission is to prepare for and respond to emergencies. Even when an EOC focuses on a single functional discipline, such as telecommunications, the incident may be caused by any number of different factors (e.g., an earthquake or a terrorist attack). In some situations, EOCs may have advance warning of an incident. For example, hurricanes and political demonstrations are often preceded by ominous weather patterns and public gatherings, respectively. In other cases, little or no warning is possible, such as an industrial accident in which toxic fumes are released.

Consequently, both the types of information available from an EOC and the categories of external information that may be useful to an EOC are driven by that primary mission—emergency preparedness and response. This section describes the categories of information EOCs typically use and suggests how that information may be useful to TMCs and FCs for purposes of operating and protecting the transportation infrastructure.

3.2.1 Information Categories

EOCs utilize both situational/operational information and record and logged information.

- Situational/operational information is used for immediate incident response and consists of:
  - Information about internal resources (i.e., the personnel and physical resources owned by, or otherwise available to, the EOC)

  - Real-time situational information provided by on-site first responders
  - Information about external resources (e.g., nongovernmental organizations such as the American Red Cross and private sector owners and operators of infrastructure elements critical to incident response, such as the telecommunications, electric power, and water delivery infrastructures).

- EOCs' records and logged information provide a record of emergency response activities and are used to both verify that procedures were followed correctly and identify lessons learned to improve future incident response capabilities. This information typically is organized in connection with after-action reports following both real emergencies and emergency response exercises.

Table 3-4: EOC Situational/Operational Information: Description and Potential Uses by TMCs and FCs

EOC Information	Potential Uses	
	TMCs	FCs
Personnel resources (e.g., available/on-call responder personnel status; available skill sets; contact information) *Physical resources for response (e.g., location, number, type, and status of response vehicles; location, availability and accessibility of supplies)*	• Resource deployment assessment (e.g., determine what demands these resources will make on available transportation infrastructure)—i.e., assess redistribution of portable DMS	• Immediate use: Support incident response • Post-incident use: Input to overall risk assessments (e.g., adequacy of staffing and deployment measures)
Real-time situational information from on-site first responders	• Assess damage, determine impact on transportation infrastructure, and coordinate applicable response efforts	• Immediate use: Support incident response • Post-incident use: Input to overall risk assessments (e.g., adequacy of staffing and deployment measures)
Information on utilities (e.g., telecommunications, power, water), such as contact information on utilities personnel, extent of damage to infrastructure, and status of restoration activities	• Assess the extent of outages/ disruptions and restoration status to determine impact on transportation infrastructure	• Immediate use: Support incident response • Post-incident use: Input to overall risk assessments (e.g., adequacy of staffing and deployment measures)

3.2.1.1 Internal Resources

Description: As described in Section 2.2: Statistics, Locations, Jurisdictions, some EOCs own and directly control their emergency response resources and others primarily coordinate, rather than own, these resources. Regardless of how an EOC is organized or funded, it will have information on the personnel and physical resources available for emergency response. This information enables the EOC to deploy the personnel, equipment, and supplies required for any given incident.

Information on personnel resources includes:

- Availability/on-call status of first responders
- Skill sets of available personnel
- Contact information for personnel.

Information on physical resources includes:

- Location, number, type, and status of response vehicles
- Availability and accessibility of equipment and supplies.

Potential Uses by TMCs: TMCs focus on ensuring the accessibility and optimization of transportation infrastructure.

- To that end, TMCs could use information regarding an EOC's internal resources to determine what demands the deployment of these resources may place on the available transportation infrastructure and whether actions are needed to accommodate that deployment. For example, an EOC may need to deploy particularly heavy equipment to respond to an incident and the most direct route to the incident site may involve crossing over a bridge that could accommodate that equipment only if no other vehicles are on the bridge. The TMC could then activate or re-deploy ITS technologies to keep other vehicles off the bridge until the heavy equipment has been transported across the bridge. If the bridge could not accommodate the equipment at all, the TMC could clear an alternate route for transporting the equipment to the incident site.
- As part of the operations of many TMCs, TMC-managed safety/service patrols are tasked to provide quick removal of disabled vehicles and debris from a traffic incident to prevent increased congestion. TMCs would benefit from being aware of EOC deployments that may be operating in locations near safety/service patrol operating areas to coordinate activities and prevent duplication of efforts.

Potential Uses by FCs: An FC could use information on an EOC's internal resources in two ways. The FC could use this information immediately to support incident response. In the longer term, the FC could use this information as input to its overall risk assessments in terms of evaluating the adequacy of personnel and physical resources and deployment measures.

3.2.1.2 On-site Situational Information

Description: First responders provide on-site situational information once they have arrived at the incident site. Such information is used to conduct damage assessments and determine the adequacy of the on-site or en route resources. This firsthand information can be invaluable, particularly when information from citizen observers or the news media is incorrect or incomplete. As a hypothetical example, a water main breaks in a central business district. The news media reported that the water at a particular location was 25 feet *deep*. In fact, the water was not 25 feet deep; rather, the water was shooting up 25 feet *high*.

The EOC would have deployed very different resources to respond to each of these two situations.

Potential Uses by TMCs: Just as the EOC used the on-site responder's information to adjust the resources it deployed to respond to this incident, the TMC in this jurisdiction would also benefit from this more accurate description of the incident. The TMC can use the information to assess damage, determine the impact on the transportation infrastructure, and coordinate response efforts. In the example above, TMC actions taken to respond to water that is 25 feet deep may have involved closing down a larger perimeter around the incident site than was really warranted in this example. The on-site situational information may also prove invaluable to notify the driving public of adverse conditions. In system-wide emergencies, EOCs and FCs could be given access to fixed and portable DMS to alert the public.

Potential Uses by FCs: FCs would use this information in the same ways as they would use the information on internal resources—to support incident response and as input to risk assessments.

3.2.1.3 External Resources

Description: External resources do not have any formal organizational relationship with the EOCs (in terms of authority or funding) but are critical to incident response. External resources may be nongovernmental organizations (e.g., American Red Cross) or resources primarily owned and operated by the private sector (e.g., telecommunication, power, and water). EOCs may maintain point-of-contact information on key decision-makers for these external resources. In addition, during emergency response, EOCs receive continuous updates from these external resources. For example, the Red Cross may provide updates on available resources and their deployment status. Public utilities may provide continuous updates about the extent of damage to the infrastructure and the status of restoration activities. Local fire and police send information to EOCs in a variety of ways depending on the jurisdiction. City EOCs would have better connectivity to real-time police, fire, and rescue operations because their scope is concentrated on the same jurisdictional area (e.g., the New York City EOC likely has extensive connectivity/monitoring of the New York City Police Department, New York City Fire Department, Port Authority Police, EMS). State EOCs are looking across the State to strategically monitor overall weather patterns and lower-level EOC activity for more significant events.

EOCs use this information to manage deployment of response personnel. For example, before first responders can enter an area where power lines are down, the power company must confirm that the electricity has been shut off to those lines so that the first responders can safely enter the area. EOCs would also use information about the expected duration of an electric power outage to make decisions about certain response activities. For example, a hospital's back-up generators may offer 3 hours of power. The EOC's response will vary, depending on when the electric company estimates that the power will be restored—the response to a 1-hour outage will be very different from the response to a 1-day outage.

In addition to providing the fundamental ability to communicate with new technologies and almost any communications device, the Next Generation 9-1-1 (NG 9-1-1) will enable location-independent call access and transfer between and redundancy of 911 centers

throughout the country once implemented nationwide. Employing an open-architecture, interoperable system of systems, NG 9-1-1 will allow these emergency communications centers to share information more quickly and with greater accuracy, and to provide access to crucial data at a level not currently available. NG 9-1-1 will also allow for information to be transmitted to the 9-1-1 call center via text, image, and video in addition to the current voice transmission function.

Potential Uses by TMCs: TMCs can use information on external resources to assess the extent of the outages/disruptions and the restoration status to determine the impact on the transportation infrastructure and the actions required to effectively manage the transportation infrastructure during the incident.

Potential Uses by FCs: FCs would use this information just as they would use the information on internal resources and on-site reports—to support incident response and as input to risk assessments.

Table 3-5: EOC Records and Logged Information: Description and Potential Uses by TMCs and FCs

EOC Information	Potential Uses	
	TMCs	**FCs**
After-Action Reports	• Gap Assessments/Lessons Learned (e.g., resources, information, or process improvements that may facilitate more effective response and recovery) • Long-term vulnerability assessments that could be used to plan infrastructure improvements	• Gap Assessments/ Lessons Learned (e.g., resources, information, or process improvements that may facilitate more effective response and recovery) • Long-term vulnerability assessments that could be used to plan infrastructure improvements

Description: EOCs typically prepare after-action reports following incidents and exercises. The after-action reports document the response activities and their effectiveness. EOCs use the report results to improve their processes, including identification and remediation of any resource gaps.

Potential Uses by TMCs: TMCs can use EOCs' after-action reports in much the same way as the EOCs use them—to conduct gap assessments and capture lessons learned (e.g., identifying resources, information, or process improvements that may facilitate more effective response and recovery activities). In addition, TMCs may use these reports to conduct long-term vulnerability assessments that could be used to plan infrastructure improvements. For after-action reports involving traffic incidents, EOC reports can be catalogued with and compared to TMC incident logs.

Potential Uses by FCs: FCs would use the information in EOCs' after-action reports in much the same ways as TMCs use such information (i.e., for lessons learned and for vulnerability assessments).

3.2.2 Summary of Transportation-Relevant Information Managed/Used by EOCs

Just as the category of information available from an EOC is driven by the EOC's primary mission of responding to adverse incidents of all types, the way in which EOC information could be used by TMCs and FCs is also driven by their respective missions:

- Although TMCs focus on the accessibility of the transportation infrastructure (rather than all infrastructures), knowledge of how the transportation infrastructure both facilitates and is affected by EOCs' incident response activities can help TMCs improve the transportation infrastructure's accessibility for incident response and identify vulnerabilities for future consideration.
- The FC's mission is to gather information from disparate sources and aggregate it to form a comprehensive, multi-dimensional perspective of the environment that informs the FC's approach to response and risk assessment. Information available from the EOCs can be a valuable complement to the other information that forms the basis of the FC's analysis, which may be used both for immediate response and for longer-term risk assessments.

3.3 Transportation-Relevant Information Managed/Used by FCs

FCs typically collect and analyze information from many available sources to produce and disseminate actionable intelligence to stakeholders for strategic and tactical decision-making. This information generally falls into the "operational" category, in regard to transportation relevance.

3.3.1 Information Categories

Just as the category of information available from an FC is driven by the FC's primary mission of collection, analysis, and dissemination, the way in which FC information could be used by TMCs and EOCs is also driven by their respective missions.

Table 3-6: FC Operational Information: Description and Potential Uses by TMCs and FCs

FC Information *For Official Use Only*	Potential Uses	
	TMCs	**EOCs**
Intelligence Alerts • *Immediate alerts within 10-15 minutes of incident* • *Limited details* • *Imminent or existing threat occurring in FC's jurisdiction* • *Includes events such as severe weather, explosions, major traffic incidents* • *Broadcast messages to predefined list of recipients (phone, pager, email distribution lists configurable by area of interest/focus)*	• Intelligence alerts that could have an effect on local transportation network	• Notify responders to stand by for a potential incident response • Determine whether/when to activate/change status of EOC (e.g., from monitoring status to partial or full activation)
Intelligence Bulletins • *Additional details beyond alert information* • *Information updates to ongoing situations* • *Less urgent, upcoming situations, special event planning and coordination* • *Can include special events such as planned protests* • *Distributed as needed*	• Intelligence bulletins that could have an effect on local transportation network • Pre-planning for special events	• Use information updates to modify EOC status and determine situation response • Use information on upcoming situations, special events to plan for such special events (e.g., augment law enforcement personnel; crowd control; pre-position medical response personnel)
Daily Report • *Daily intelligence gathered from open source and classified sources* • *Global and regional impact* • *Standard format* • *International, local* • *Published at end of day* • *Typically distributed via email, may be posted to portal*	• Interested in incidents that could have an effect on local or regional transportation network	• Interested in incidents that may affect the community or infrastructure within the EOC's jurisdiction
Intelligence Reports • *Usually the day after a situation* • *Large-picture, macro analysis of major incident* • *After-action reports*	• Use for lessons learned (changes to staffing and physical resources; process improvement) and input for future exercises	• Use for lessons learned (changes to staffing and physical resources; process improvement) and input for future exercises

FC Information *For Official Use Only*	Potential Uses	
	TMCs	**EOCs**
Threat Assessments • *Annual* • *Quarterly* • *Incident-specific* • *State of Affairs or Annual Threat Assessment, inclement weather season preparation, major construction impact* • *Distributed usually via email*	• Near-term threat assessments that could affect mobility on the transportation network including: – Increased congestion – Transit delays – HazMat – Evacuation routes • Long-term threat assessments can be used for infrastructure and ITS planning	• Use information for near-term planning (e.g., staffing levels, availability of physical resources) • Use information for long-term planning (e.g., budgeting for additional staffing/physical resources)

3.3.1.1 Intelligence Alerts

Description: Intelligence alerts can address both imminent and existing threats that occur in an FC's jurisdiction. These alerts can contain many types of information, from incoming weather, to an explosion occurrence, or a major traffic incident. This information can come to the FC from any source (e.g., police officer on the street, transportation agency work crews, news agencies). First reporting is usually limited and may not be completely reliable. However, the alert gives an initial warning to supporting agencies for awareness and immediate response or preparation, depending on the incident.

The intelligence alerts are usually sent out within 10 to 15 minutes of an incident being discovered and are usually broadcast to a predefined list of recipients either via phone, pager, or through an e-mail distribution list that is configurable by the area of interest or focus. The alerts are sent out to first responders and agency partners through a tiered system for dissemination of information. Agencies outside the first responder tier can also be included on the alert distribution list if they are regularly involved with emergency response (e.g., transportation officials and emergency management officials). The individuals within these agencies who receive these alerts are screened to verify their suitability to have access to sensitive information[44] and their need to know such information. In most cases, these individuals are senior-level officials or cooperating law enforcement and first responder agencies who have responsibility for initiating response activities.

As is normally the case, the originator of the information will send it to his/her contact lists. In turn, an agency on that contact list will forward the message to its contact list. In many cases, there will be redundant messaging. However, as FCs receive information on an incident from many different agencies, they fuse these differing reports and data through analyses and then disseminate the information based on a more complete understanding of the incident.

44 They may have security clearances or the agencies may have conducted some level of background investigation on them to verify their trustworthiness.

Potential TMC Uses: TMCs are interested in any information that would affect mobility on the transportation infrastructure. TMCs often collect their own information about the incidents and special events that could affect the transportation network. However, intelligence alerts from an FC would benefit a TMC because there might be some information that the TMC has not yet received; it also serves as a way to verify information from an additional source.

Potential Uses by EOCs: An EOC could use information from intelligence alerts in two ways:

- To notify responders to stand by for a potential emergency
- To determine whether/when to activate or change the status of the EOC (e.g., from monitoring status to partial or full activation).

In some cases, the FC's jurisdiction may not be congruent with the EOC's jurisdiction. For example, the FC's geographical jurisdiction may include multiple EOCs, but the incident that provoked the intelligence alert may not require a response from all of the EOCs. In such cases, this information is most immediately useful to the affected EOC. However, the information may also be useful for the other EOCs if the incident has the potential to affect their jurisdictions or if the affected EOC may need personnel or physical resources as mutual aid from those EOCs not currently affected. A wildfire is one example where this could be the case. The resources needed to contain the fire may exceed those available to the affected EOC, and it is certainly in the best interests of the surrounding EOCs to help the affected EOC contain the fire so that it does not spread to their jurisdictions. The intelligence alert would also allow those unaffected EOCs to begin to position themselves to respond if the fire spread into their jurisdictions and take actions such as sending text messages to volunteer firefighters to be prepared to respond if needed.

3.3.1.2 Intelligence Bulletins

Description: Intelligence bulletins follow alerts and are issued as the FC gathers more information, validates information already provided, and continues to track the progress of the ongoing incident. In addition to providing updates regarding ongoing incidents and special events, these bulletins can contain updates and information on upcoming situations, special event planning and coordination, and planned protests. These bulletins are distributed as needed to those agencies and individuals that have been identified as having a need to know or have a focus, and operate, in that particular area of interest. (This list of recipients will usually be the same as the recipients of the initial alert, with possible additions as the situation dictates.)

The additional details provided by an FC beyond the alert information can provide first responders and support agencies with a clearer operating picture. The bulletins include analysis of a situation as it has unfolded and has been tracked by the FC's professional analysts. The FC will normally continue to issue intelligence bulletins until the incident has reached closure and will send out a final bulletin notifying recipients of a closed incident.

Potential TMC Uses: TMCs would value continued updates on activities affecting the transportation infrastructure. Information on planned special events could support pre-planning

activities. Additional details would increase the reliability of the decision making regarding transportation infrastructure.

Potential Uses by EOCs: EOCs could use information updates from intelligence bulletins in two ways:

- EOCs could use information on ongoing situations to modify the EOC status and determine how to respond to the situation
- EOCs could use information on planned special events to determine what measures are needed to prepare for the special event (e.g., augment law enforcement personnel, implement crowd control measures, and pre-position medical response personnel).

Using the example of a wildfire, the additional details and updates about an ongoing incident would allow the affected EOC to refine its response and would allow the potentially affected EOCs to determine whether the fire was advancing in a way that warranted modifying their status from "monitoring" to "activating."

With respect to information in intelligence bulletins regarding planned special events, the EOCs could take actions such as informing personnel that they may not schedule vacation during the timeframe within which the special event will occur or renting equipment (e.g., such as crowd control fences) that may not ordinarily be readily available.

3.3.1.3 Daily Report

Description: FC daily reports consist of daily intelligence based on both open source (newspapers, television news, partner agencies, etc.) and classified source information. These reports are published at the end of every day and are distributed to all of the FCs across the country and other recipients. This information is usually transmitted via e-mail or may be posted to a secure portal. Reports reflect information that has both regional and global impacts because anything could be of relevance and could impact the ongoing analysis process. Both local and international trends are shared with other centers to help with ongoing investigations, highlighting a trend, or just simply providing awareness of a situation. The reports also include any threat to a particular infrastructure that has a regional or nationwide impact. Each FC follows its own standard format for these reports, but formats may vary among centers.

Potential TMC Uses: TMCs would value continued updates on activities affecting the transportation infrastructure. Additional details would increase the reliability of decision making.

Potential Uses by EOCs: Daily reports contain information that has both global and regional impact. An EOC would use a subset of this information, specifically any information about incidents or special events that may affect the community or infrastructure within (or perhaps adjacent to) its jurisdiction. Such information may inform the EOC's monitoring activities for the following day.

3.3.1.4 Intelligence Reports

Description: Once an incident is closed, the FC analysts will begin reconstructing the incident from its inception to closure to compile an intelligence report. Intelligence reports

are usually issued the day (or week) after an incident. Not to be confused with after-action reports, the intelligence reports provide analysts and partner agencies with a large-picture overview, or macro analysis, of a major incident or special event that has just occurred. Intelligence reports can be shared across the country with other FCs to share best practices or lessons learned. These reports can also be used to strengthen overall operations and procedures and will include detailed information about the incident as well as provide an analysis of how the incident pertains to the area of responsibility, a particular critical infrastructure, law enforcement, or national security. Intelligence reports also provide valuable input to quarterly and annual threat assessments.

Potential TMC Uses: As with after-action reports, intelligence reports involving traffic incidents can be catalogued along with, and compared to, TMC incident logs to assess the effectiveness of the response and implement necessary SOP revisions.

Potential Uses by EOCs: EOCs could use the information in intelligence reports much as they use information from their own after-action reports (e.g., to identify changes required in personnel and physical resources or processes and as input for future exercises). For example, if the intelligence report identified deficiencies in staffing, physical resources, or response processes, the EOC could remediate those deficiencies and then use the incident addressed in the intelligence report as the scenario for the exercise. This would test whether the deficiencies had been adequately remediated. If not, the EOC could identify additional measures required. Further, EOCs can even benefit from after-action reports about incidents in which they may not have been involved—they can factor the lessons learned elsewhere into their own exercises and planning.

3.3.1.5 Threat Assessments

Description: Each FC develops periodic threat assessments for the locality under its jurisdiction. These assessments are used to generate the State of Affairs or an Annual Threat Assessment—reports that can be presented to the Governor of the State and any other officials who have a need to know this information. These reports contain information on topics such as inclement weather preparations, major construction impacts, the overall jurisdictional threat assessment, critical infrastructure assessments, and evacuation planning and preparation. Typically, these assessments are distributed via e-mail, but presentations are also made as requested. A threat assessment can offer insight about the jurisdiction's vulnerabilities and operational capabilities. Legislators and agencies can use this information to focus resources to mitigate vulnerabilities identified in the report and identify ways to enhance the jurisdiction's operational capabilities to respond to an incident or special event.

Potential TMC Uses: TMCs would find any threat assessments useful that would affect transportation infrastructure. Threat assessments affecting mobility could improve the TMC's situational awareness and allow it to focus current efforts on the most critical threats. In the case of a transportation-related threat, TMCs could use threat assessments to prepare or position resources to deal with threats that would increase congestion or delay transit operations. For example, if a threat is related to the release of hazardous materials on or near roadways, TMCs could begin to implement precautions to protect travelers and

develop alternate routes. If a major threat is imminent that would involve the evacuation of citizens from an area, the TMC could use the advance warning to begin setting up evacuation routes, to include preparing for traffic control activities such as reverse lane flow operations. Long-term threat assessments can also benefit the TMCs by identifying vulnerabilities of the infrastructure and ITS resources, which TMCs could use for planning purposes.

Potential Uses by EOCs: EOCs could use threat assessments in two ways:

- Incident-specific threat assessment information would be useful for near-term planning.
- Longer-term threat assessment information would be useful in long-term planning, such as developing budgets and identifying capital projects that may be required to develop capabilities to adequately respond to emerging threats. For example, a State of Affairs Report might reflect that our adversaries are becoming interested in attacking the water delivery infrastructure. The EOC may then need to explore how to respond, addressing issues such as the location of alternate sources of water, the quantity of water available, and orderly distribution methods.

From the EOC perspective, intelligence alerts, bulletins, and reports are generally of greater interest than the daily reports and threat assessments.

Along the axis of *immediate versus long term*, the EOCs focus most of their efforts on immediate situations. They certainly also have longer-term interests. For example, they conduct exercises to better prepare themselves to respond to future incidents and, just as all organizations, they need to be forward-looking in terms of their budgets and evolving in concert with their environment. However, their primary day-to-day mission is to respond to immediate incidents.

Along the axis of *local versus national*, EOCs focus most of their efforts on those factors that affect the geographical jurisdictions (or, in some cases, the functional disciplines) for which they are responsible. They are concerned with situations beyond their immediate jurisdictions or functional disciplines primarily to the extent that more global incidents or special events may materialize. This could directly affect their areas of responsibility, or offer lessons learned in case similar emergencies or special events affect their areas of responsibility in the future.

In contrast, FC products such as daily reports and threat assessments tend to have a long-term, big picture, global focus, reflecting:

- How a discrete incident or special event may impact the more global situation
- How a global situation may impact the local environment
- How a situation affecting one infrastructure component/functional discipline may affect another.

3.3.2 Summary of Transportation-Relevant Information Managed/Used by FCs

The category of information available from an FC is driven by the FC's primary mission, and by information security and privacy constraints. But as FCs collect, analyze, and then disseminate information, it is also important to understand that information sharing is one of the key components to the viability of an FC.

Arizona Department of Transportation

Arizona Traffic Operations Center

CHAPTER 4. CHALLENGES AND OPTIONS FOR INFORMATION EXCHANGE

This chapter provides an overview of key challenges and barriers to information exchange among centers, as well as alternatives to overcome them. The chapter discusses center policies and regulatory issues, technical challenges, and potential solutions.

Primarily, the communications and data management capabilities needed to address information-sharing are within today's state of the art. Appendices E and G of this report address the reliability, security, and vulnerability of the information sources, data transmission channels, and equipment.

When analog television converted to digital television on June 17, 2009, the 700 MHz spectrum that broadcasters owned for that purpose was no longer needed. That spectrum was turned back to the Federal government to allow the Federal Communications Commission (FCC), the Federal agency that manages the spectrum, to begin the process of reallocating the spectrum. In July 2007, in advance of the conversion to digital television, the FCC revised the 700 MHz band plan and service rules to promote the creation of a nationwide interoperable broadband network for public safety and to facilitate the availability of new and innovative wireless broadband services for consumers.

During the summer of 2009, following the conversion, the National Interoperability Information eXchange (NIIX)[45], as part of the National Public Safety Telecommunications Council (a federation of organizations whose mission is to improve public safety communications and interoperability through collaborative leadership) through their Governance and Operations Working Groups, has developed definitions and other material to help define who should be included to use the national interoperable broadband wireless spectrum.

This chapter primarily focuses on three topics—privacy, security, and (on the technical side) data integration and vulnerability.

4.1 Center/Stakeholder Policies and Regulatory Issues

One of the key challenges facing the centers' ability to exchange information revolves around policy and regulatory issues.

4.1.1 Information Technology (IT) and Data Management Policy

Policy issues that often present roadblocks to information exchange in specific cases include:

45 See National Interoperability Information eXchange, http://www.niix.org/niix/index.jsp, accessed 2010.

- Organization-wide IT/security and firewall policies that have typically been tailored to specific agency or more broadly held policies (e.g., statewide) to prevent or limit external access to sensitive databases
- Contracts and agreements with commercial interests or other agencies on the use and dissemination of information with financial or other value to these interests/agencies
- "Ownership" and liability for the proper use and cost of misuse of information, which is provided with the expectation that it is valid and appropriate for the intended use.

4.1.2 Privacy

Two key laws impact the ability for these centers to exchange information—the Privacy Act of 1974, Public Law 93-579, and title 28 Code of Federal Regulations (CFR) Part 23. This section includes a discussion of these laws, as well as the limitations and concerns they impose on the centers.

The Privacy Act of 1974, Public Law 93-579, states:

> No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains…[46]

Broadly stated, the purpose of the Privacy Act is to balance the Federal Government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their *privacy* stemming from Federal agencies' collection, maintenance, use, and disclosure of personal information about them.[47]

28 CFR Part 23 regulates operating policies for all domestic organizations receiving Federal funding for criminal intelligence systems. 28 CFR Part 23, most recently updated in 2001, defines a criminal intelligence system as "the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information."[48] This definition is now applied to FCs. It also governs the basic requirements for the intelligence system process. This process includes:

- Information submission or collection
- Secure storage
- Inquiry and search capability
- Controlled dissemination
- Purge and review process.

46 U.S. Department of Justice, *Privacy Act of 1974*, http://www.justice.gov/opcl/privacyact1974.htm, accessed 2010.

47 U.S. Department of Justice, 28 CFR Part 23, http://www.cops.usdoj.gov/default.asp?Item=172, accessed 2010.

48 U.S. Department of Justice. 28 CFR Part 23, Criminal Intelligence Systems Operating Policies. 1998.

This regulation recognizes that certain crimes (e.g., drug trafficking, smuggling) involve some degree of coordination and permanent organization over a large geographical area. 28 CFR Part 23 acknowledges that pooling information about such activities is necessary but could represent a threat to the *privacy* of individuals. It is reported that the US DOJ now trains FCs on 28 CFR Part 23 twice a year to assure compliance.

As an example of the reach of Part 23, in 2002, the Americans Civil Liberties Union (ACLU) filed a class action lawsuit against the Denver Police Department when it was found to have collected and retained information on non-criminal elements (American Friends Service Committee v. City and County of Denver). The lawsuit filed by the ACLU against the police involved in the sharing of this intelligence information challenged the monitoring and recording of peaceful citizens. The ACLU also stated in its suit that the police falsely labeled its clients as "criminal extremists." Those so labeled apparently included peace activists and education and human rights organizations, suspected as possible threats to public safety. Mayor Webb came out following the lawsuit to say that Denver police had gone too far, compiling "intelligence files" on 3,200 individuals and 208 organizations that demonstrated no credible threat. The Mayor also ordered all intelligence records be archived at the Denver Public Library and "preserved for study." Part of this archive is available to the public (copies of newspaper clippings, pamphlets, flyers, articles, and photographs). Restricted files are now made available only to persons or organizations named in the files until 2055, when all files will be released to the public.

For TMCs, privacy issues are often cited as a key challenge. While the TMC primary function does not include law enforcement, the information gathered and monitored by the TMC can assist law enforcement officials. However, some TMCs, such as those operated by the Virginia Department of Transportation (VDOT),[49] state, for example, that their field equipment is incapable of identifying license plates of passing traffic and that they do not record video feeds. The Rhode Island Department of Transportation[50] asserts that its TMCs maintain a camera system privacy policy, where their operators are instructed to: "(1) Only focus the cameras on the highway and highway related areas, and (2) Only zoom into an accident scene to determine incident response needs and then zoom out to monitor traffic flow." Additionally, cameras are "blanked out" on the Web site and cable channel when they are being used in responding to an incident.

In addition, there are potential privacy and liability concerns when handling 9-1-1 calls. In March 2002, the 511 Deployment Coalition published *Deployment Assistance Report #2, Transfer of 511 Calls to 911*, examining the issue of a 511 system receiving a call intended for 9-1-1 and what concerns there may be for the 511 system to transfer the call to 9-1-1. While there are some technical issues to overcome to allow the transfer to happen, the report states, "In order to transfer a call to a 911 center, the carrier must provide the callers Automatic Identification Number (AIN). While it is technically feasible for the carrier to provide this information, they will be hesitant to do so because of *privacy* concerns and other State legal considerations." In addition, there may be liability concerns because "511

49 Jeff Sturgeon, "VDOT regional traffic management center has Virginia roads covered," Roanoke.com, November 29, 2007, http://www.roanoke.com/news/roanoke/wb/141528, accessed 2010.

50 State of Rhode Island Traffic Management Center, FAQs, http://www.tmc.state.ri.us/faqs.asp, accessed 2010.

operators, both public and private, are concerned that they could face potential liability if, for example, a call transferred to a public safety answering point ("PSAPs"), the facilities that answer 911 calls for emergency assistance, is dropped during the transfer or the call is directed to a PSAP located further from the caller than another PSAP. Under these or similar scenarios, a caller needing emergency assistance could suffer an aggravated injury or, at worst, death if the 511 call center fails to transfer the call properly."

4.1.3 Classified Information

Issues also exist concerning the classification of information. Personnel within FCs are aware of the different types of information that they are both handling and disseminating from the FC. This information can be public, sensitive, or secret. Classification types will determine how each piece of information is shared, not only with outside agencies but also among the agencies operating within the FC itself. Over-classification can present operational challenges when personnel are not able to read or pass information because the source has classified the information at a level that makes information sharing across the normal lines of communication difficult.

4.1.4 Legal Process and Rules of Evidence

When there is a potential for surveillance information and transactions like 9-1-1 calls to contain evidence that could be relevant to ongoing investigations and/or legal proceedings, enforcement agencies (and many FCs) are very cautious about release, alteration (such as redaction of *privacy*-sensitive information), chain-of-information "ownership," verification, and security of information used and retained. Therefore, while it may make operational sense for an FC to receive or provide transportation-related information, this exchange can be handicapped—because the required standards of reliability and verification may be higher than practical for TMCs to meet. In comparison, practical limits exist for TMCs because they gather real-time or near-time data for (usually) non-emergency operational purposes and can, in most situations, tolerate some reliability issues because of redundant information sources and assets in the field.

4.1.5 Training Needs Assessment

TMC personnel may be called upon to physically serve in an EOC or FC to provide on-site subject-matter expertise in support of incident management activities. Preparing personnel for this type of work requires training that may be different from information analysis training or other technical training relevant to the person's primary position.

In assessing the training needs of EOC and FC support personnel, the functional requirements discussed in the previous section must be mapped to training needs to meet these requirements. As discussed, the functional (and thereby training) requirements differ between the EOC and FC, with EOC requirements being more widely recognized than those of the FC. Appendix H includes an inventory of training resources.

4.1.5.1 Emergency Operations Centers

EOCs are typically staffed 24 hours per day by a dedicated watch responsible for monitoring potential or actual emergency situations in a given jurisdictional area. When certain threats emerge and reach a level that requires EOC "activation," an "event team" or "incident management team" is activated and responds to the EOC to support a multi-agency, cross-functional response and recovery effort.

A large portion of the event or incident management team is comprised of predetermined ESFs, with ESF positions filled by pre-designated personnel from the ESF lead department or agency. In the case of ESF-1, personnel are typically assigned from within the jurisdiction's transportation department, and sometimes fill this position as a collateral duty assignment. Whether a full-time or collateral duty assignment, ESF-1 personnel have specific training needs based on the nature of the ESF-1 role in overall emergency management.

Training needs must be mapped to specific requirements that are determined by overall training mandates and specific training needs based on function. In emergency management, the standardized training mandates can be traced back to Homeland Security Presidential Directive - 5 (HSPD-5), *Management of Domestic Incidents*, in which the development of NIMS is mandated. Published in 2004, NIMS provides "a consistent nationwide approach for Federal, State, and local governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity." Further, as directed in HSPD-5, NIMS includes "a core set of concepts, principles, terminology, and technologies covering…training; …and qualifications and certification" in order "to provide for interoperability and compatibility among Federal, State, and local capabilities."[51]

As further described in NIMS:

> Incident management organizations and personnel at all levels of government, and within the private-sector and nongovernmental organizations, **must be appropriately trained** to improve all-hazards incident management capability nationwide. Incident management organizations and **personnel must also participate in realistic exercises**—including multidisciplinary and multijurisdictional events and private-sector and nongovernmental organization interaction—to improve integration and interoperability. **Training involving standard courses on incident command and management, incident management structure, operational coordination processes and systems**—together with **courses focused on discipline-specific and agency-specific subject-matter expertise**—helps ensure that personnel at all jurisdictional levels and across disciplines can function effectively together during an incident.[52] [Emphasis added]

Designed for Federal, State, local, and tribal governments, as well as the private sector and nongovernment organizations, NIMS serves as a means to effective coordination in emergency response and recovery operations. As such, all levels of government are encour-

51 The White House, Homeland Security Presidential Directive 5.

52 U.S. Department of Homeland Security, *National Incident Management System*, March 2001, p. 43.

aged to adopt NIMS through a formal process called NIMS Implementation, which outlines particular implementation steps for all levels of government and nongovernment sectors. Since most EOCs are operated at the State and local levels, the *NIMS Implementation Matrix for States and Territories* and the *NIMS Implementation Matrix for Tribal and Local Jurisdictions* provide the necessary guidance. Developed and issued by the NIMS Integration Center under FEMA, the matrices serve as a guide for specific jurisdictions to use in developing and executing NIMS-compliant preparedness and operational programs and functions.

Because transportation sector personnel would serve in an EOC as part of the interagency emergency coordination effort in support of the ICS during a response and recovery operation, transportation entities would need to ensure that assigned personnel meet the documented training and exercise requirements as outlined in the relevant matrix. Further, due to the nature of the work performed at the EOC, most EOC SOPs require that assigned personnel be employees of the represented agency with decision-making authority on behalf of that agency. These criteria, as they pertain to training requirements, indicate that assigned personnel serve, at a minimum, as middle managers within their agencies. This is important, as training requirements are based on management level and command authority of personnel.

In studying both the State and local matrices, it was concluded that the same compliance criteria exist for preparedness training and exercises as they relate to both State and local workers. As previously cited, there are two areas of training required under NIMS:

- Standard courses (which address the NIMS requirement for incident command and management, incident management structure, and operational coordination and systems)
- Discipline- and agency-specific subject matter expertise.

In fulfilling the "standard courses" requirements, transportation personnel assigned to the EOC must meet the following criteria as outlined in the matrix documents:

- Complete IS-700, NIMS: An Introduction
- Complete IS-800, National Response Plan: An Introduction
- Complete ICS-100, Introduction to the ICS
- Compete ICS-200, ICS for Single Resources and Initial Action Incidents
- Complete ICS-300, Intermediate ICS for Expanding Incidents
- Participate in a multi-discipline, multi-jurisdictional all-hazards exercise.

In addition, self-study is available through the FHWA's *Simplified Guide to the ICS for Transportation Professionals* published in February 2006.

These training activities would prepare the discipline-specific specialist for support operations in the EOC environment. As such, it is assumed that the ESF-1 designee will have completed appropriate discipline- and agency-specific subject matter training, and will have gained expertise in required areas.

4.1.5.2 Fusion Centers

FC intelligence analysts are trained in law enforcement and intelligence disciplines. As part of their professional responsibilities, general intelligence analysts may be assigned to focus areas such as critical infrastructure and transportation as part of the strategic mission on countering terrorist activity. As such, transportation specialists are typically not assigned to an FC. Further, general intelligence analysts assigned to cover critical infrastructure and transportation sectors have immediate access to specific transportation centers, agencies, and personnel through interagency collaboration based on case needs.

As previously described, many FCs are operated by the principal State law enforcement agency, and are geographically located as a stand-alone operation. Many other FCs are co-located with the State TMC. In situations where the FC is not co-located, general intelligence analysts employed at the FC focus on transportation sectors as part of their overall responsibilities, and may call upon transportation industry experts for input and advice as required. In the co-location environment, FC and TMC personnel work closely on a regular basis, providing information and support daily.

Regardless of the location of the FC, transportation personnel may at some point be called upon to provide direct support to FC operations based on need and area of expertise. To adequately support FC mission requirements, transportation personnel must understand the law enforcement and intelligence environment to fully understand and provide for the mission. As such, adequate basic training on law enforcement intelligence processes is warranted. When transportation experts understand the law enforcement intelligence and analysis process, they will be better equipped to provide relevant and timely information and data that could be vital to the intelligence fusion process.

4.1.6 Training for TMC Personnel Working in EOCs and FCs

4.1.6.1 EOCs

Based on the functional and training requirements for transportation personnel working in an EOC, it is recommended that TMCs, or other appropriate transportation agencies, develop a training and certification program for emergency transportation personnel. The training program should be NIMS compliant in that personnel should be trained and certified in their respective areas of expertise. However, it is important that personnel assigned to EOCs complete the additional training and exercise participation to be fully competent in emergency operational support roles. Specifically, training for transportation specialists should include courses that provide an overview of the emergency management industry; the ICS; and the nation's strategy for preparing for, responding to, and recovering from major incidents or disasters.

Such training may include independent study courses provided by the Emergency Management Institute, covering instruction in NIMS, NRF, and ICS.

4.1.6.2 FCs

The transportation industry is a key element in counter-terrorism and disaster response operations. As a target, the transportation infrastructure requires ongoing monitoring and

protection; and as a critical element of the supply chain, the transportation infrastructure needs to be operationally maintained to support the U.S. economy and serve as a means for moving critical resources during disaster operations.

Transportation agencies must ensure that interagency coordination and collaboration with FCs are established and utilized. Such efforts will ensure that relevant information is shared with appropriate entities in a timely manner and will further solidify the cross-jurisdictional and cross-functional partnerships necessary for countering criminal and terrorist activities. Because interagency coordination is largely relationship-based, transportation agencies should designate a core group of technical experts that will collaborate with FC personnel on an ongoing basis. Similar to the ESF-1 emergency operations assignments, designated transportation specialists assigned to support intelligence operations may establish interagency relationships with State law enforcement and intelligence offices and personnel and gain general awareness of their functions and operational needs.

In preparing transportation specialists for assignments in support of law enforcement and intelligence operations, transportation agencies also need to ensure that personnel receive adequate awareness and training that will enhance support capabilities to law enforcement and intelligence operations. Specifically, transportation specialists should attend and participate in basic criminal intelligence operations, intelligence analysis, and anti-terrorism awareness and training. Most available courses are short in length, but provide the appropriate level of awareness for State and local personnel supporting multi-agency intelligence operations.

Unlike NIMS in the emergency management industry, the law enforcement and intelligence industries do not currently offer prescribed training packets for interagency liaison personnel. As such, individual States and FCs, in particular, must develop specific requirements for liaison officers based on available resources that meet the needs of the organization.

4.2 Technical and Vulnerability Challenges

Enabling the use of information in centers' legacy information management systems and processes represents a key challenge for the exchange of information among TMCs, EOCs, and FCs. Key issues include the standards for correct interpretation and use of information by receiving centers, capacity and bandwidth of communications resources typically available to centers, and the reliability and vulnerability of needed information, both routine and especially in connection with incidents.

4.2.1 System Integration, Message Standards, Language

Thirty regional agencies in the Philadelphia area that are determined to establish an integrated regional information-sharing network have been facing a major challenge. One of the most challenging barriers is the development, agreement, and implementation of data and message standards, a location-referencing framework, and terminology system that would support rapid transfer of information between agency practitioners and legacy systems that do not otherwise function with compatible information structures. There are parallels with the TMC, EOC, and FC information-sharing initiatives addressed here because

the participating agencies have long-established systems of organizing, parsing, interpreting, and using data in ways needed for their unique purposes and for their unique missions.

"Open" access to information (in this illustration, video feeds) presents coordination issues for users and providers, too. In Delaware, one of these issues was discovered when the TMC cut off one of its traffic cameras that was able to view a State police bomb squad operation. Unknown to the TMC, the State police bomb squad, at their own location during the incident, were viewing the movement of their remote bomb squad robot via a public Web site that had that camera online. When the TMC cut the feed, the State police were no longer able to see the robot. The TMC and the State police did not know that there was no other way for the State police to access that feed once it was cut.

Ideally, a permanent command and control center would serve every disaster area. The center would have all of the necessary equipment and enough independent power sources to not be dependent on local infrastructure. However, having a permanent operations facility at every possible disaster area is neither feasible nor recommended.

Instead, a mobile and/or rapid deployment facility is more cost effective and scalable. For example, Broward County, Florida, has a Mobile EOC/Command Post Vehicle. The vehicle was purchased at a price of $500,000 with Federal funds and has the following features:

- Conference area
- State-of-the-art interoperability radio communication system, which provides connectivity to different radios with multiple frequencies
- Weather station
- Satellite Internet capability
- Satellite telephone
- Multiple cell phone ports
- Wi-Fi computer capability
- GIS capability
- Direct TV
- Multiple plasma screens for viewing video and video conferencing
- Remote-controlled outside cameras for monitoring and surveying.

The vehicle took 6 months to complete and has a Freightliner body and chassis.

4.2.2 Vulnerability

ITS can be vulnerable to a variety of disruptions, both naturally occurring and man-made, such as extreme weather, floods, earthquakes, power outages, hazardous material incidents, fire, and intentional attack. To ensure uninterrupted functionality of ITS technologies, it makes sense to plan for such situations. This can involve the design and implementation of

back-up systems that duplicate or support some of the most important functions needed; planning for a large-scale community-wide incident; and management, testing, and documentation for backup systems to ensure their functionality in case of primary system failures.

Appendix G of this report addresses technical considerations for planning and implementing vulnerability improvements for ITS.

4.2.3 Unique FC Issues

FCs have unique information-sharing issues. Issued in August 2006, the FC Guidelines were designed to help law enforcement, public safety, and private partners come together with a common purpose and to improve their ability to protect the homeland and prevent crime. The working group that was established to develop the FC Guidelines developed 18 areas of guidance. These areas include:

- The National Criminal Intelligence Sharing Plan and the Intelligence and Fusion Processes
- Mission Statement and Goals
- Governance
- Collaboration
- Memorandum of Understanding (MOU) and Non-Disclosure Agreement
- Database Resources
- Interconnectivity
- Privacy and Civil Liberties
- Security
- Facility, Location, and Physical Infrastructure
- Human Resources
- Training of Center Personnel
- Multidisciplinary Awareness and Education
- Intelligence Services and Products
- Policies and Procedures
- Center Performance Measurement and Evaluation
- Funding
- Communications Plan.

Despite offering guidance in these areas to both new and already established FCs, an October 2007 GAO report on FCs still found that there were issues reported concerning interoperability, clearances and classification, training, and the sustaining of operations.

The push for Federal intelligence information sharing and law enforcement information sharing led to the existence of FCs. In spite of this, a long-standing issue for FCs continues to be interoperability and interagency communication of information. Integration of information systems among the Federal, State, and local government and tribal communities continues to be a major technical challenge. These issues exist not only when FCs try to communicate data with Federal, State, local, and tribal partners but also from FC to FC. In some cases, centers may not be equipped to handle classified material or may not even have staff cleared to the necessary levels to receive certain information.

FCs have also reported having issues trying to receive training and guidance from DHS and U.S. DOJ. At issue are the standards that should be set for analyst training as well as information-sharing policies and procedures. These issues can present technical challenges for the FCs as well. Training shortfalls, such as a lack of a standardized nationwide training program for analysts, impact the ability to have effective communication among centers. When centers are unable to receive guidance on information-sharing policies and procedures, they are not able to properly identify shortfalls and gaps that may exist in the fusion process or the methods of sharing and gathering information.

As a supplement to the guidelines created in 2006, DHS's I&A clarified the role that FCs would play in the intelligence process and the support that the Federal government would provide by issuing the *Baseline Capabilities for State and Major Urban Area Fusion Centers* outlined in Table 2-3.

The I&A seeks to create an environment in which federal resources are aligned to assist FCs in achieving their goals through promoting partnerships, enhancing the lawful sharing of information, and coordinating interactions between Federal, State, and local resources through communication, collaboration, understanding, coordination, and management support:

- DSS seeks to ensure efficient and effective ***communication*** with FCs by creating the Single Point of Service (SPS) to ensure that all inquires are responded to expeditiously by the appropriate elements within DHS and developing other communications tools, including the Homeland Secure Data Network (HSDN), the Homeland Security Information Network (HSIN), and the HSIN-Intelligence portal—to improve communications with FCs.
- New guidelines also enhance ***collaboration*** through partnerships that deepen connections among analysts with expanded collaborative analysis, assessment, and planning capabilities including with fire service, public health, and emergency management personnel.
- The I&A has also implemented programs to increase ***understanding*** of agency capabilities and needs through expanded partnerships, including needs recognition and training programs.

- DHS also seeks to improve ***coordination*** by continuing to develop processes and tools to increase the transparency of activities and information exchanged with the FCs.
- By establishing a baseline level of capability for all FCs through the *Global Fusion Center Guidelines,* the *Office of the Director of National Intelligence – Information Sharing Environment Implementation Plan*, and the *Interaction with State and Local Fusion Centers Concept of Operations*, the I&A seeks to integrate support programs and provide ***management support*** across DHS, DOJ, and other government entities.[53]

In a Statement for the Record on March 4, 2010, before the U.S. House of Representatives Subcommittee on Homeland Security, Caryn Wagner, Undersecretary for Intelligence and Analysis for DHS, recognized the need to continue to share intelligence and information and strength relationships between the I&A and the State and local FCs.[54]

4.2.4 System Ownership and Funding

Centers of all three types frequently encounter policy and political issues with ownership and investment costs associated with information sharing—particularly when funding for significant information-gathering systems (e.g., ITS) and communications systems have been justified by a center's specific mission and provided by a specific agency. Centers are typically held accountable for the value produced by those investments and for deploying systems that are specifically fit for the purpose of the funding agency's objectives.

At the same time, one of the frustrations by political entities and the public is on the redundancy of equipment, which has in part resulted from the ownership and funding issues identified above. During the spring 2007 meeting of the National Conference of State Legislatures, members expressed frustration at the U.S. DOT and DHS due to their mounting of surveillance cameras at the same locations but not sharing the information/images from the cameras. However, there are examples of coordinated camera image sharing such as the 2008 Republican National Convention in Minneapolis - St. Paul when the Minnesota DOT, the two local police departments, capital security, and the transit agency shared images from their 900 individual camera systems and broadcast them into both a traffic control center and the multi-agency communications center.

4.3 General Options and Principles to Address the Challenges

Overcoming the challenges and barriers addressed above will depend on the determination of both partners in any specific information exchange initiative—and their "political will" to revisit key policy and rules interpretations and to invest in the technical solutions needed. This, plus the inevitable investment of management attention, effort, and money, suggests that TMCs, EOCs, and FCs should study the needs and opportunities and carefully select their first initiative to pursue. ***Initial focus should be on selected information***

53 U.S. Department of Homeland Security, *Interaction with State and Local Fusion Centers, Concept of Operations*, December 2008.

54 U.S. House of Representatives Subcommittee on Homeland Security Statement for the Record, Caryn Wagner, Undersecretary for Intelligence and Analysis for the Department of Homeland Security. March 4, 2010.

exchange solutions that are clearly needed, with benefits that can be convincingly demonstrated. This focus, of itself, is a formidable challenge.

4.3.1 IT and Data Management Policy

Many long-standing IT policies and rules are candidates for review and updating in light of the continuing development of firewall and secure communications technology. For example, one State agency (following its IT policy) did not permit one of its TMCs to connect to the State network because of the existence of other "open" Web-based applications being employed at the TMC.

Solutions can be found in clear definitions of information and appropriate use, security needs justified and defined, interagency MOUs, compartmentalization of sensitive data, and effective tools for secure communication available today.

4.3.2 Privacy

Each organization that shares information resources must have its own policies and procedures to comply with Federal, State, local, and tribal privacy laws. Processes and agreements are needed to assure that information transmitted is limited in form or content to conform to the policies of both organizations. Information that contains or might contain surveillance data should be covered in agreements to forms and content that comply with both organizations' policies. Uses of such data should be specified, as well as the users authorized to access the data.

4.3.3 Classified Information

Transmission of classified information "in the blind" is neither practical nor lawful. This is a major barrier to sharing of classified information. The options are few. Two options are: (1) to require special handling, redaction, or processing to truncate information to exclude the classified information, or (2) to encrypt the transmission and ensure that access on the receiving end is only by properly cleared and authorized personnel (including methods to vet the actual identity of those persons) and that appropriate control can be maintained in the receiving facility. Both approaches are expensive.

The first approach (redaction/truncation) requires labor-intensive, time-consuming effort by cleared personnel, or very sophisticated programming and technology, and a secure facility. This approach generally compromises the value and timeliness of the information finally transmitted.

The second approach (encrypted transmission to cleared entities) also requires investments in facilities, technology, and properly cleared personnel—if not already available at the receiving center. If the information is properly received and secure, there would still be the potential for the value of the data to be reduced if only part of it can be passed on to uncleared operators or decision-makers at the receiving center.

4.3.4 Legal Process and Rules of Evidence

The options for transmitting information that is—or *could* become—part of a legal process are fairly similar to the two options for classified data, with some additional hurdles. In this case, the restrictions needed may not be fully known or understood prior to the completion of an ongoing investigation, or until all subsequent legal processes are completed. Determining this would require expertise in law enforcement and legal process and possibly court orders.

Information that is public knowledge and otherwise recorded facts or qualified observations could probably be exchanged freely—but again, significant effort by qualified experts would be needed to "scrub" the exchange.

4.3.5 System Integration, Message Standards, Language

By leveraging technology, centers can begin to address some of the technical and vulnerability challenges described in the previous section. These technology solutions include interconnection equipment, database, middleware, integration, and business intelligence tools. But the best approach to developing and integrating these technologies is to implement solutions that utilize industry standard products, services, and processes.

The U.S. DOT encourages the use of the National Transportation Communications for ITS Protocol (NTCIP) and other related standards for ITS implementations. For FCs, U.S. DOJ encourages the use of industry standards including the Global Justice XML Data Model and the National Information Exchange Model (NIEM). The approach to successful information sharing includes the use of XML data models, the Common Alerting Protocol messaging standards, and service-oriented architectures.

With transportation departments seeking to emphasize corridor management and emergency preparedness, a document-centric single delivery information method poses several problems when broadcasting information to all parties regardless of relevance or appropriate level of detail, leading to circular reporting and information overload. A new trend in TMC traffic and fleet management systems is the development of automated decision support systems. New enterprise systems provide rapid information collection from not only their own devices and equipment but also from diverse network sources that can meet the center's needs.

4.3.6 Vulnerability

Vulnerability to loss of operational effectiveness or continuity is a concern for all of the center types addressed in this guidebook. Whether damage to operations is direct (resulting from natural events, accidents, or intentional acts) or indirect (resulting from unforeseen technical problems or loss of utility support), the acceptable tolerance vulnerability varies considerably. In other words, the amount that each center is willing to spend to reduce vulnerabilities has to be a practical choice by type, category, and mission criticality of each center.

With practicality in mind, the most common measures for coping with vulnerability and operational continuity risks involve redundancy of systems, facilities, and supporting utilities. Common redundancy measures fall along a spectrum of investment, as follows:

- Fully redundant and operational back-up systems and facilities
- Redundant "hot sites" with back-up system equipment (non-operational, often shared)
- Shared (usually) "cold sites" with space, utilities, possibly furnished
- Cooperative agreements to utilize, work with, or shift functions to other operational centers.

Each of these general approaches has different implications on cost, operational continuity, recovery, and robustness of interim services. Appendix G of this report discusses these measures further.

4.3.7 Unique FC Issues

For many of the reasons cited earlier (security classification, privacy, legal process issues, etc.), FCs have had to cope with significant barriers to information exchange and interoperability with other FCs—not to mention TMCs and EOCs.

As a result, FCs have typically communicated via specifically prepared products, including alerts, bulletins, reports, and situational/risk assessments. This approach has obvious implications for the timeliness, detail, and value of information in some of the products, but it can facilitate direct communication with properly cleared decision-makers.

Appendix E of this report provides more information on these issues.

4.3.8 System Ownership and Funding Issues

Solutions to the policy and political issues with ownership and investment costs associated with information sharing must be addressed by agencies in an objective way, with thoughtful exposition (from the viewpoints of each center/agency) of the relative need and both the value and the cost of meeting the need, as well as the savings benefits of sharing some or all of the cost. A simple example of two centers deploying video resources at a common location illustrates this:

- Center "A" requires a reliable, fixed video camera feed at a specific location, at 5-minute intervals to fill an important gap in traffic flow observation. This camera costs $3,000.
- Center "B" requires a reliable camera with additional resolution and other functionality. This specification takes about $6,000 to meet.
- Both centers have determined for their needs that the respective investments are justified by the cost of the respective cameras.
- Both centers agree that the more expensive system could be shared operationally and could meet the needs of both centers.

- Center "A" agrees to pay one-third ($2,000) of the cost, thereby saving $1,000.
- Center "B" agrees to pay two-thirds ($4,000) of the cost, thereby saving $2,000.
- Assuming Center "B" needs included movable surveillance, the automated routine could return to the traffic surveillance position every few minutes to send a feed to meet the needs of Center "A."
- On the (rare) occasion of an incident in the viewing range, Center "B" may have to train the camera and interrupt the regular traffic feed for a short time.

This simplistic scenario implies what some of the typical operational policy compromises might involve to better enable sharing of information and information-gathering resources, as well as to minimize the cost. The implications of this example also show how the benefits and needs for information exchange have to be considered objectively from the points of view of each entity involved in the exchange.

Frisco, California Fire Department

Frisco, California Emergency Operations Center

CHAPTER 5. LESSONS LEARNED AND SUCCESSFUL PRACTICES

This chapter provides a compilation of lessons learned and successful practices based on case and field research. The focus of the research and findings presented is on exchange opportunities, solutions to exchange barriers, and benefits gained.

Interagency exchange of information promotes rapid, efficient, and appropriate response from all agencies. Public safety agencies benefit from obtaining closed-circuit television pictures for verification and assessment of an incident as they begin their response. This visual information helps the agencies to dispatch the appropriate response teams and to recall those teams if the incident clears up before they arrive. Public safety agencies can also benefit from information regarding traffic conditions on the response route and special information, such as blocked railroad crossings or construction that might affect the response.[55]

5.1 Lessons Learned

The *Computer-Aided Dispatch (CAD) – Traffic Management Center (TMC) Field Operational Test: (FOT): State of Utah Final Report*[56] provides lessons learned on the field test conducted that aimed to integrate the Utah Highway Patrol (UHP), the Utah Department of Transportation (UDOT), Salt Lake City Fire and Police Departments, the Utah Transit Authority (UTA), and the Valley Emergency Communications Center (VECC) information systems to enable the real-time exchange of incident data. The FOT documented lessons learned, which include:

- **Involve IT staff early in the project planning process.** Interviewees mentioned the importance of involving agency IT staff early in the development of the integrated system. This is important so the IT organization provides technical input to the system to assure that the computing and communication environments fit within each agency and can be effectively maintained.
- **Understand the importance of close working relationships from the start.** All of those interviewed by the Evaluation Team mentioned the importance of the close working relationship among the agencies involved in this FOT. The work these agencies did in preparation for and during the 2002 Winter Olympic Games strengthened the close working relationship. Although not every region can strengthen relationships among agencies by hosting the Olympic Games, agencies should consider how to build these relationships in advance of implementing an integrated system.

55 Transportation Research Board, NCHRP Report 20, *Sharing Information between Public Safety and Transportation Agencies for Traffic Incident Management*, 2004.

56 U.S. Department of Transportation, Intelligent Transportation Systems, *Computer-Aided Dispatch – Traffic Management Center Field Operational Test: State of Utah Final Report*, U.S. DOT ITS Program Assessment Support Contract, July 2006.

- **Provide dedicated staff working on integration, or staff with emphasis on integration.** Interviewees mentioned that it was often difficult to spend enough time on the integrated system. Decisions and work items sometimes took longer than those involved would have preferred. Even though every agency supported the integrated system, staff had normal responsibilities with integration duties added on. It would be ideal if staff involved had a priority on the integrated system tasks.
- **Build in short development cycles to reduce staff turnover issues.** Interviewees mentioned that some agencies had critical staff turnover during the implementation of the integrated system. Staff turnover can be disruptive to implementation schedules and budgets as new people have to come up to speed on the system. If the system is planned to have incremental implementations (see Section 4.2: Technical and Vulnerability Challenges), then the development cycles for each incremental implementation can be short to minimize the likelihood that staff will turnover during a given development cycle. Staff turnover between cycles is not as disruptive as turnover during a development cycle.
- **Understand the importance of considering the role of business practices in the integrated system.** As discussed earlier in this document, it is important that the integrated system not require a change in the operator's or dispatcher's work process. However, if other aspects of an agency's business practice would improve the integrated system, it should be considered. For example, VECC agencies were concerned about providing certain information to the integrated system. UDOT is planning to develop an MOU with the VECC agencies that will specify how the information will be used. This may allow a change in those agencies' business practices that will lead to more information shared in the integrated system.
- **Understand the importance of coordination meetings.** Interviewees mentioned the importance of ongoing, periodic coordination meetings with the partner agencies. These meetings kept communication open and emphasis on the integrated project.
- **Define what data is exchanged and when.** In the Utah system, the IEEE 1512 standard was selected for incident management messages and codes. However, not all vendors supported those codes. It is important for agencies to prepare for differences in codes and determine how to handle these differences.
- **Decide what incidents will be shared among agencies and what information will be exchanged when an incident is shared.** The experience in Utah is leading the participating agencies to automatically send incidents of interest and allow the receiving systems to filter those incidents to display the ones that are likely to be of most interest to the operators.
- **Understand the importance of incremental implementation.** In the Utah system, agencies learned a lot in the initial implementation of the integrated system. The agencies are using that knowledge to plan improvements to the integrated system. For agencies planning an integrated system, it is recommended that they plan an initial implementation and at least one subsequent, incremental improvement. Any group of agencies is almost certain to learn how they would prefer to have the system operate.

The project and related contracts should be arranged to allow the agencies to implement what they learn in the initial implementation.

- **Understand the importance of redundant communication path.** As discussed in Section 4.3.6, a back-up communication pathway is important. Agencies should plan to include redundant communications in an integrated system.
- **Minimize or avoid duplicate entry**. Because not all needed information is transferred from the VECC to the integrated system, the UDOT operators have to enter data in their system that was already entered by VECC dispatchers in their system. Ideally, any given piece of information would only be input once by any operator in the integrated system. This is an important concept to plan for in any integrated system.

Information sharing across agencies promotes a strong basis for collaboration and coordination in managing incidents. Much evidence in case studies on operational performance benefits is anecdotal and has not been formally quantified. For example:

- Incident responders in San Antonio have estimated that joint training and planning activities of the TMC have resulted in a 40-percent decrease in incident clearance times.
- The Washington State Department of Transportation (WSDOT) has developed a quarterly reporting process to track various performance and accountability measures for routine review by the Washington State Transportation Commission and others. The report includes a section on incident response, including the total number of responses by month, the average clearance times by month, and the number of incidents that lasted more than 90 minutes.

A challenge in identifying operational performance benefits was generally a lack of baseline performance data from which to measure.

The FOT conducted by Utah also provided a summary of the benefits that may be achieved through the CAD and TMC system integration. Benefits cited in the study included:

- **Enhanced field operations associated with locating and responding to incidents.** To a significant extent, Utah previously realized this benefit. UDOT and UHP had previously co-located staff at TMCs, and CAD terminals were placed in TMCs to enable data sharing. The most significant benefit realized by the project was the ability to engage in direct data exchange between legacy systems, rather than having an operator observe two or more terminals. This real-time exchange of data adds to the benefits previously obtained through interagency cooperation, represents an additional enhancement of field operations, and fills what had been a gap in the existing incident management and response program already in place in Utah.
- **Geo-location for placing incidents and marginal improvement in scene clearance.** Observed benefits included the use of Geo-location in providing a mechanism to place incidents without operator intervention, and from interviews, a qualitative assessment that scene clearance time seemed to improve marginally. Better traveler information offers the public the opportunity to bypass the incident, which leads to less congestion

and better response sooner (response units getting to the scene via a clear route). This logic seems sound; however, data was not available to support these conclusions.

- **Enhanced communications among responders; enhanced on-scene activities.** The evaluation was not able to completely assess this benefit. The system is newly deployed and, while operational, is still undergoing refinement. This benefit would be more accurately assessed when the system has matured and has been in use for a period of several years instead of several months.
- **Enhanced efficiency in documenting the incidents.** In the first 2 months of operation, the number of incidents documented by the integrated system increased by about 800 percent. The number of incidents for which the TMC maintained data increased significantly after the CAD-TMC integration. The main difference observed between the before and after data discussed above was that UDOT seemed to maintain much more complete incident records after the deployment, both in terms of the number of incidents recorded and the details recorded about each incident. It is believed that this increase is due in large part to the fact that CAD data was more readily available to TMC operators after the CAD-TMC deployment. This is supported, in part, by the large number of incidents in the after data for which Dispatch Services/9-1-1 were listed as the reporting agency.
- **Improved data quality.** The electronic data collection, particularly in recording the incident start and stop times, has significantly improved overall data quality. An additional example of this is reflected in a decrease in the error rate for the coding of incidents by type.
- **Improved interagency working relationships.** Utah had already achieved substantial progress in this area, and the project represented a continuation of this benefit. Utah's success in this area is represented by the interagency discussions on the amount and type of data that should be exchanged between the systems; the interagency cooperation that enabled this data exchange established the venue for addressing this type of system refinement based on initial deployment experience.
- **Enhanced communication with the traveling public and media.** This benefit would be more properly addressed at system maturity. While anecdotal evidence obtained during after-project interviews indicates that enhanced communication is occurring, assessing this metric based on several years of implementation experience will provide a more accurate measure of the benefit of enhanced communication to the traveling public and the media. From observations, efficiency in documenting incident management improved. Input for some fields was automated so the UDOT operators did not have to enter this data.

According to a June 10, 2009, article in the *Salt Lake Tribune*, "New System Aids Communication in Emergencies," the system is now finishing the testing phase allowing incidents to be instantly shared electronically. "It also includes a mapping program that provides real-time displays of incident locations and resources deployed, which will improve communications and ensure efficient use of resources, officials said."

A 2006 companion report, *Computer-Aided Dispatch – Traffic Management Center Field Operational Test: Washington State Final Report*, was also prepared and contains conclusions and recommendations that can be of value to other agencies considering such a system.[57]

The FHWA funded FDOT's *i*Florida project to test a number of ITS applications including TMC, 511, and CAD integration. The i*Florida Model Deployment Final Evaluation Report*[58] included three lessons learned during the test including:

1. **FDOT should work with the Florida Highway Patrol (FHP) to ensure that practices are in place to enter key information needed by FDOT in the correct fields within the CAD system.** The data needs of FHP were different from those of FDOT, so some data fields that were key to FDOT but not key to FHP were not always entered consistently. One example was the road name, which was sometimes entered in the FHP CAD system as part of the free text description rather than in the road name field. FHP cooperated closely with FDOT by encouraging its dispatchers to follow more stringent data entry requirements with respect to these fields.

2. **Transferring data from the FHP CAD system required translation of some coded values from FHP's values to those recognized by FDOT.** An example was the incident type. Because FHP sometimes revised the list of acceptable values for incident types and their meanings, FHP instituted procedures to ensure that the tables used to translate FHP incident type values to FDOT values would be updated whenever such changes occurred.

3. **Event-driven messaging is subject to errors related to dropped messages.** A system that uses event-driven messaging should include methods for identifying and recovering from dropped messages.

5.2 Successful Practices

This section provides examples of how centers are currently sharing information and the barriers that exist to successful information sharing, as well as a discussion of the processes that enable it.

5.2.1 Case Examples of Information Sharing

The Transportation Research Board (TRB) report (see footnote at the beginning of Chapter 5 of this guidebook) defines four primary means of information sharing:

- **Face-to-Face.** Encompasses direct interpersonal activities, usually at joint operations or shared facilities

57 U.S. Department of Transportation, Intelligent Transportation Systems, *Computer-Aided Dispatch – Traffic Management Center. Field Operational Test: Washington State Final Report*, 2006, http://ntl.bts.gov/lib/jpodocs/repts_te/14325_files/index.htm, accessed 2010.

58 U.S. Department of Transportation, Federal Highway Administration, iFlorida Model Deployment Final Evaluation Report, 2009, http://ops.fhwa.dot.gov/publications/fhwahop08050/chap_5.htm, accessed 2010.

- **Remote Voice.** Includes common communications options such as telephones and land mobile radio
- **Electronic Text.** Involves text messaging via paging, facsimile, or email devices and text access to traffic incident-related data systems, including CAD
- **Other Media and Advanced Systems.** Comprises technology-dependent methods not addressed in previous categories, such as video and other imaging systems, and integrated technologies such as advanced traffic management systems.

The study found that the primary means of center-to-center interagency communications remains standard wireline communications. Where transportation centers operate freeway management systems by CCTV or other video systems, embedded sensors in roadways, DMS, and HAR systems, the information generated by these systems is readily shared with co-located public safety officials. In some cases, control of these systems is shared remotely.

In the case of the Kentucky Intelligence FC (KIFC) and the State TOC, both operations are not only housed in the same building but operate out of the same room. Operations are kept separate, allowing TOC staff to not need national security clearances. However, staff do undergo a thorough background check before they are able to work in this tightly secured facility.

The facility itself was assessed once it was built, and it was determined that the space, along with the common threads between the centers, warranted their co-location. While there might be a clear division between centers, there is no hesitation between center staff to share information. Any TOC data that is recorded (e.g., back-ups, crashes, other incidents) is posted to the Internet and is available to anyone who needs access to the data, including FC staff. The State Police Vehicle Enforcement Unit, formerly an operation run by the State DOT, continues to maintain its station at the TOC for coordination purposes. Vehicle Enforcement and the TOC share information through CAD. However, because the KIFC and the TOC work in the same facility, besides CAD, much of the information exchange is informal. Conversations, e-mails, and phone calls are the primary methods used to exchange data as needed. Currently, the TOC has 179 traffic cameras in the State and 38 DMS, with most of them controlled out of the TOC. For the KIFC staff, access information that can be provided by these traffic cameras or the ability to have messages posted on DMS is literally just a few steps away. It is also important to point out that while none of the TOC and KIFC systems are linked, staff at both centers feel that there is still a very good flow of information.

Table 5-1: Summary of Information-Sharing Methods by Surveyed Public Safety Entities[59]

Location	Face-to-Face	Remote Voice	Electronic Text	Other Media and Advanced Systems
Albany, NY	Two co-location sites	Some sharing of public safety radios; some use of commercial wireless service "talk groups"	Shared CAD system	Roadway data, images, and video shared remotely
Austin, TX	Co-location site ready to open*	Safety/service patrols equipped with local police radios	CAD data to be shared remotely	CCTV control shared with local police
Cincinnati, OH	Transportation center hosts regional incident management team operations	Some sharing of public safety radios; some use of commercial wireless service "talk groups"	Shared CAD under development	CCTV and other traveler information are shared with public
Minneapolis, MN	Multiple co-location sites	Shared radio systems; some use of commercial wireless service "talk groups"	Shared CAD data	CCTV and other traffic management systems are shared
Phoenix, AZ		Safety/service patrols equipped with local police radios; shared radio system to be deployed	State DOT data workstations provided to local public safety agencies	CCTV shared with local fire department
Salt Lake City, UT	Co-location site	Safety/service patrols equipped with local police radios	Shared CAD data	CCTV and other traffic management systems are shared
San Antonio, TX	Co-location site	Safety/service patrols equipped with State patrol radios; center-to-center intercom system	Shared CAD data	CCTV and other traffic management systems are shared
San Diego, CA	Co-location site		Shared CAD data	CAD data are posted on traveler information Web site

59 Transportation Research Board, NCHRP Report 20, *Sharing Information between Public Safety and Transportation Agencies for Traffic Incident Management*, 2004.

Location	Face-to-Face	Remote Voice	Electronic Text	Other Media and Advanced Systems
Seattle, WA			Shared CAD data	Control of CCTV is shared with State patrol

* Combined Transportation Emergency Coordination Center (CTECC) is operational

Another example of successful information sharing came about when a "hot truck," a truck suspected of carrying radiological materials, alerted a sensor at a weigh station in Laurel County, Kentucky, that it may be carrying a radiological substance. Since this vehicle was not supposed to be carrying such material, the State police vehicle enforcement desk, located in the TOC, was immediately notified of the situation. As the vehicle was intercepted by State police units, the KIFC worked to gather all available intelligence on the vehicle, the driver, operating company, manifest, etc. The KIFC staff worked through the TOC and vehicle enforcement to provide the officers on the scene with all of the relevant information necessary so that they were able to safely and successfully handle the situation.

The KIFC and State DOT representatives were quick to point out that while these operations may have been unique at the time, the way the incidents are handled together has become part of their day-to-day coordination activities.

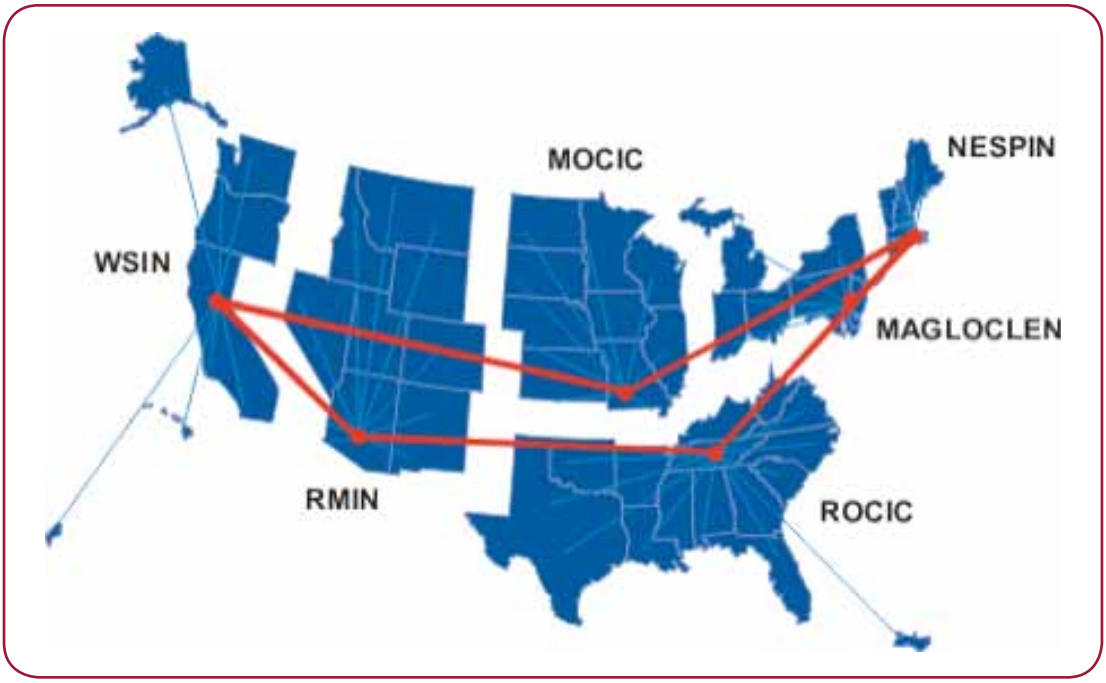
Another example of information sharing is in the District of Columbia metropolitan area, which includes the collaboration of the District, Maryland, and Virginia DOTs. Information, incident response responsibilities, and evacuation plans are all shared via the Information Sharing and Collaboration Capabilities program and the Regional Integrated Transportation Information System (RITIS), with the regional TMC as the central command center.

Many FCs across the country are members of the RISS. FCs, such as the Delaware Information Analysis Center, use this system for information-sharing purposes. According to its Web site, RISS is a national program of regionally oriented services designed to enhance the ability of local, State, Federal, and tribal criminal justice agencies. The focus of RISS is rapid information exchange for criminal activities; however, RISS also offers training to member States and enhances information sharing.

RISS is broken into six regional centers, as shown in Figure 5-1:

1. **MAGLOCLEN** – Middle Atlantic-Great Lakes Organized Crime Law Enforcement
2. **NESPIN** – New England State Police Information Network
3. **MOCIC** – Mid-States Organized Crime Information Center
4. **WSIN** – Western States Information Network
5. **RMIN** – Rocky Mountain Information Network
6. **ROCIC** – Regional Organized Crime Information Center.

Figure 5-1: RISS Regional Centers[60]



While criminal information sharing is the overall focus of RISS, other pieces of information are exchanged to enhance the quality of the analysis and to provide useful information to other partners.

5.2.2 Approaches to Overcoming Institutional, Operational, and Technical Barriers

Where the TRB report found the greatest successes in information sharing, formal frameworks have served as the cornerstone for those successes. The frameworks stem from broader regional cooperative efforts and include regional traffic management or incident management organizations. Examples include:

- In **New York State**, the relationship between the Thruway Authority and the State police epitomizes public safety and transportation integration. At the Thruway State Operations Center, TIM (Transportation Information Management) information sharing between public safety and transportation is seamless; single individuals serve as the nexus for both agencies. The seamless integration is made possible by transportation funding of State police operations and by Thruway Authority employees serving as public safety dispatchers.
- **San Antonio** region organizations established a TMC in the 1960s to address regional transportation management issues. As the importance of managing traffic incidents has increased, the TMC has proven to be an effective mechanism for fostering communication and coordination among responders. The TMC consists of

60 Regional Information Sharing Systems (RISS). Institute for Intergovernmental Research Website. http://www.iir.com, accessed 2010.

representatives from the Metropolitan Transit Authority, the San Antonio Public Works Department, Alamo Dome, the San Antonio Police Department, the Bexar County Sheriff's Department, EMS providers, towing and recovery service providers, and county health agencies.

- **Washington State Patrol (WSP) and WSDOT** have cooperatively developed a joint operations policy statement. The purpose of this working agreement is to document the joint policy positions between the two agencies regarding issues of mutual interest in operating State highways. As a result, both agencies are able to make decisions internal to their own agencies to provide the foundation that ultimately supports information sharing between the two agencies.
- **Minnesota DOT** and State police have established multiple MOU and guidelines since 1999 that lay the groundwork for coordinated TIM and interagency information sharing.
- **Salt Lake City** established closer working relationships between transportation and law enforcement in the region. Early in the process, the senior leadership in both departments signed a memorandum of agreement between their respective agencies. This expression of commitment and support proved to be an effective tool for bringing the members of each department closer together. The close working relationship was evidence that the spirit of the agreement was emphasized in the following years by senior and mid-level management in both departments, and it has come to be regarded as a native and natural way of doing business together.

Utah's field test aimed to demonstrate how the integration of CAD and TMC systems could improve incident response capabilities and how institutional barriers could be overcome.[61] Utah's technical approach was intended to include the following elements and perform the associated functions:

- **Create a common message set**, structured in a uniform and open format, to enable the exchange of information among multiple agencies with unique requirements, policies, and operating environments. Two interagency shared data messages (ISDM) are planned—the interagency service requests (ISR) and the interagency Advanced Traffic Management System (ATMS) message (IAM). The ISR specifically requests services rendered by public safety agencies and secondary responder services. ISRs may be between CAD systems and/or between CAD systems and ATMS to specifically request public safety and secondary responder services. The IAM relates to traffic condition advisories and traffic control requests between CAD systems and the ATMS.
- **Support the ISR via data specification sets (DSS)** that incorporate the standard data elements found in all CAD systems. The DSS will specify an XML application to import and export (I/X) the data sets. The DSS will also specify the data standards for each element, as per the Institute of Electrical and Electronics Engineering (IEEE) standards, including IEEE 1512-2000, 1512.1, and 1512.2, as available and applicable. The ISR-DSS specifications will be in the public domain.

61 U.S. Department of Transportation, Intelligent Transportation Systems, *Computer-Aided Dispatch – Traffic Management Center Field Operational Test: State of Utah Final Report*, U.S. DOT ITS Program Assessment Support Contract, July 2006.

- **Select a commonly used operating system and language** (e.g., Windows 2000 and Visual Basic) to develop legacy system interfaces (LSIs) between existing UHP and UDOT systems to enable information exchange. The LSI will be a stand-alone server program in the public domain designed for nationwide application at TMCs for the ISR and IAM messages between different vendor CAD systems and between CAD systems and ATMS.
- **Develop LSIs between the State systems and county and municipal government systems** (VECC, Salt Lake City).
- **Integrate the new UTA CAD system** currently under development.
- **Continue UDOT ITS Division-developed unique browser-based Event Tracking System (ETS) to manage and update planned events** (e.g., roadway construction), and in real time for subsequent dissemination to the traveling public. The ETS is being deployed statewide, and will be used by local city, county, and State agencies. Information from the ETS will be updated and integrated into the CommuterLink traffic management system, including 511, using XML.

5.2.3 Training Examples

Overall, TMCs, FCs, and EOCs typically do not engage in cross training or analyst exchanges. However, States involved with RISS have the opportunity to engage in conferences that provide both training and information sharing. This section provides a discussion of TMC training findings as well as the differentiated training needs of FCs.

According to a U.S. DOT study, *Transportation Management Center Concept of Operations, Improving Transportation Network Efficiency*, training of staff is critical for ensuring successful TMC operations. In a survey of eight key centers, the report details training operations and procedures for three sample centers—Boston, Toronto, and Atlanta. Innovative training and documentation procedures observed include Boston's plans for online procedures, Toronto's "functionally" oriented help function, and Atlanta's use of hypertext in help and training materials. The following are excerpts from the study's findings on training.

- Boston—due to the constantly changing condition of its road network because of the construction of the Central Artery/ Tunnel—has a program of continually updating its procedures.
- Toronto has reorganized its operations department to include an individual assigned to maintain and update its procedures, and Atlanta has created a training and documentation staff within its operations department. Atlanta has also created a position in its ITS organization for document control.
- Because of the frequent change of its procedures, Boston has implemented desktop rehearsal and new and altered procedure simulations to ensure operational readiness.
- Atlanta periodically assigns its operators to accompany the services they support and interact with, such as the motorist assistance patrol. Atlanta's training program offers examples of several valuable practices. Atlanta has established a training unit in its planning department, which prepares operations procedures. New operators begin with

a 2-week formal training program on the operator console and software and progress to 3 to 4 days each of training on various duties, procedures, and response plans. New hires are provided tours of the project area to gain familiarity with the road network and device locations. They also ride with the motorist assistance patrol during their new-hire training.

Although it was not one of the three centers whose training operations and procedures were specifically studied in the report, the study reported that staff at Wisconsin DOT's MONITOR program in Milwaukee recognized the need for a different orientation in the training of its law enforcement partner and they developed a customized training manual for its use. Milwaukee has provided a system workstation at the law enforcement dispatch site and has received positive feedback from the law enforcement dispatchers regarding this access.

Topics of training specifically for FCs focus on a different set of skills, and can include anti-terrorism training, crime-specific investigative techniques, surveillance techniques, use of specialized equipment, officer safety information, and analytical techniques.[62] A specific example of the development of a training program at an FC is the Michigan Intelligence Operation Center (MIOC). While awaiting DHS to finish development of its field training for intelligence and information sharing, MIOC has begun to develop and offer various forms of training for local law enforcement and partners of the intelligence cycle. The MIOC considers public safety and private sector components of the fusion process to be its partners in the intelligence cycle. To the MIOC, these components represent nontraditional gatherers of information, and it views their interaction as opportunities to enhance and increase the amount of information that is shared. The MIOC has developed a recommended list of Federal training programs for its partners' consideration; however, some of the training may not be available to agencies unless they can be sponsored by a local law enforcement entity.

5.3 TMCs, EOCs, and FCs Working Together

The intent of this section is to provide detailed examples of where TMCs, EOCs, and FCs are currently working together, the strategies employed to facilitate the information exchange, and the benefits gained through collaboration.

The first examples provided include a discussion on information sharing and collaboration in Kentucky and New Jersey. The KIFC and the State TOC provide insights into coordination through the use of technology. Officials at the joint KIFC and State TOC stated that they coordinate efforts to track shipments when nuclear/radiological materials are moved from Oak Ridge National Laboratories to the depleted uranium hexafluoride conversion facility (DUF6) in Paducah, Kentucky. KIFC staff will use the TOC cameras to track the movement of the shipment while the TOC staff supply route information and updates.

62 Regional Information Sharing Systems (RISS), Institute for Intergovernmental Research Web site. http://www.iir.com, accessed 2010.

The New Jersey Regional Operations and Intelligence Center (ROIC) and the MIOC not only function as traditional FCs, but also act as the statewide operations center during an incident. Richard Cañas, director of New Jersey's Office of Homeland Security and Preparedness, suggests using FCs in emergency response: "[it] may be a concept that could be a model for other states."[63] In the event of a school shooting, for instance, the ROIC facilitates a seamless flow of information between the various agencies that would be responding.[64] The center's 100-seat facility can project live aerial footage, building blueprints, and hospital locations onto its 32-foot screen, which all partner agencies can work from to coordinate their efforts.

Table 5-2 provides specific examples on observed best practices for integration that illustrate how TMCs, EOCs, FCs, and other transportation agencies have successfully worked together during incidents.

Table 5-2: Observed Best Practices for Emergency Integration[65]

Best Practice	Locations	Observed Implementation
Placement of TMC workstations in related EOC – Technical Integration	Houston TranStar	Location of regional EOC in the same building as the TMC allows data networks to be connected, giving EOC workstations full access to TMC data resources
	Austin Combined Transportation, Emergency and Communications Center (CTECC)	Location of regional EOC in the same building as the TMC allows data networks to be connected, giving EOC workstations full access to TMC data resources
	Georgia NaviGAtor	Location of the TMC on the same campus as the statewide EOC allows placement of a TMC workstation connected to the NaviGAtor system in Atlanta with full functionality
	Maryland Coordinated Highways Action Response Team (CHART)	Connection of the statewide emergency management center to the CHART system using ATM protocols on commercial communication infrastructure gives the CHART workstation at the EOC full functionality and acceptable video quality

63 Regional Information Sharing Systems (RISS), Institute for Intergovernmental Research Web site. http://www.iir.com, accessed 2010.

64 Council on Foreign Relations, Eben Kaplan, Fusion Centers, February 22, 2007, http://www.cfr.org/publication/12689/, accessed 2010.

65 U.S. Department of Transportation, Federal Highway Administration, *Integration of Emergency and Weather Elements into Transportation Management Centers*, February 2006.

Best Practice	Locations	Observed Implementation
Establishment of interagency agreements at management level – institutional integration	Houston TranStar	Formal agreements among local and State government agencies carrying signatures from high-ranking officials covering establishment, funding, management, and operations of the combined center
	Austin CTECC	Formal agreements among local and State government agencies carrying signatures from high-ranking officials covering establishment, funding, management, and operations of the combined center
	Orlando Florida Department of Transportation (FDOT) D5	A general MOU establishes an organizational structure and documents commitment for information sharing and implementation coordination
Implementation of a data network on publicly owned infrastructure and available only to regional cooperating agencies – technical integration	Orlando FDOT D5	Installed fiber owned by individual consortium members is interconnected to establish a region-wide Ethernet network private to the consortium used for sharing video, data, and remote server access
	Salt Lake City	Installed fiber is interconnected with local partner agencies to establish a region-wide Ethernet network private to the agencies used for sharing video and data
Co-location of operational agencies – physical integration	Houston TranStar	Co-location of primary operations site of State DOT district operations, transit dispatch, and transit police along with representatives from regional police, traffic operations, and commercial traffic reporters allows pooling of resources and establishment of familiarity among staff members from all agencies
	Austin CTECC	Co-location of operations site for several organizations in the facility housing multi-agency EOC brings benefits in availability of resources and familiarity of staffs to emergencies requiring an activation of the EOC
Restricted access Web site – technical integration	Pennsylvania Turnpike	Access from the TMC and other authorized organizations to a Web site operated by the Pennsylvania Emergency Management Agency allows for a two-way flow of highly accurate incident information with higher reliability to the Web site than publicly available Web sites provide

Best Practice	Locations	Observed Implementation
Regular interaction among agencies when responding to localized emergencies – operational integration	Pennsylvania Turnpike, Austin, Orlando, Houston, Salt Lake City, CalTrans D7, Maryland CHART	Many of the centers encourage staff interaction on both a task basis and a casual basis to foster working relationships among staff members. The most common interaction is between TMC staff and law enforcement, but also can include emergency medical, fire, transit, and hazardous materials agencies.

The following provides a more detailed discussion of examples from Boston, Houston TranStar, and Kentucky.

5.3.1 Boston – Integrated Project Control System (IPCS)

The Boston IPCS is an integrated traffic management and tunnel systems control application for Boston's 7.5-mile central artery and tunnel system. The system is operated by the Massachusetts Turnpike Authority (MassPike) out of its Operations Control Center (OCC). The OCC also works with the 511 service; Smart Routes; other transit and traffic agencies including the Massachusetts Bay Transportation Authority (MBTA), Massachusetts Port Authority (Massport), and MassHighway; and the City of Boston. The control center works very closely with other agencies and emergency services including the State police, local fire departments, EMS, towing services, and roadway maintenance to provide up-to-the-minute communication on travel conditions and incident response.[66] Boston IPCS found that, once established, public and other agencies began to depend on IPCS services, regardless of internal or external pressures that developed. To satisfy this consistent demand, Boston IPCS has implemented several redundant computer systems to ensure operation even if the primary computer fails. In Boston, other agencies depend on the information that Boston IPCS is able to provide. Additionally, computer systems provide traffic management functions and life-critical functions such as ventilation and fire control in area tunnels. To achieve this, Boston runs hot backup systems, so that the loss of the primary system does not result in the disruption of the entire system. The system also distributes its processing among multiple sites, so that functions from malfunctioning processors can be allocated to others. In June 2009, Governor Deval Patrick signed a bill creating the Massachusetts Department of Transportation (MassDOT) that combines MassHighway, MBTA, MassPike, and the Registry of Motor Vehicles. MassDOT began operations on November 1, 2009. According to the mass.gov website, "transportation employees working together have co-located the MassPike OCC and the MassHighway Traffic Control Center in a single facility. Tobin Bridge traffic cameras were also redistributed to the combined facility in South Boston. From this single location, operators of the State's bridges, tunnels, and surface roadway systems can now share images and information and communicate directly regarding incidents that may impact different operations.

The communications link between the Tobin Bridge and OCC required the installation of cable including a video and data link to provide operational efficiencies in roadway safety, security, and event response. The combined OCC is staffed 24 hours a day to monitor sev-

66 See Massachusetts Turnpike Authority, http://www.masspike.com/bigdig/background/occ.html.

eral major State highways and facilities and detect and report incidents with more than 630 cameras."[67]

5.3.2 Houston – TranStar

TranStar is a multi-agency TMC that provides traffic management, traveler information, and emergency management to the Houston metropolitan area. To facilitate collaboration, the center hosts law enforcement staff from both Houston Metro and Harris County in a control room. These officers participate in special event planning including special event execution and coordination. Additionally, Houston's EOC is also co-located within the TMC. Communication is facilitated to allow each agency to focus on its skills, resources, and primary purpose in any situation, resulting in faster consensus.

5.3.3 Frankfort, Kentucky TOC

The Frankfort, Kentucky TOC is a multi-functional center that collects and disseminates traffic and highway incident information to the traveling public. The TOC has implemented an extensive email notification system to relay information to stakeholders around the State, including weather watches and warnings as well as real-time traffic incident information. Additionally, an Office of Homeland Security-mandated FC is co-located in the same center, allowing multiple agencies with different specialties to pool resources to respond to a variety of threats. During a special event or incident, representatives from the Department of Highways; Homeland Security Offices; Kentucky State Police; Kentucky Vehicle Enforcement; FBI; Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); Kentucky National Guard; and Kentucky EOC each have the opportunity to join staff at the TOC to address relevant issues, having access to TOC resources and information.

Jeff Sangillo

Kentucky Emergency Operations Center

67 See Massachusetts Department of Transportation, "MassDOT Reforms: Traffic Operations Control," http://transportation.blog.state.ma.us/blog/2009/10/massdot-reforms-traffic-operations-control.html, accessed 2010.

Chapter 6. SUMMARY – ASSESSING THE VALUE OF TMC/EOC/FC INFORMATION-SHARING

TMCs face on a daily basis the demands of making fast operational decisions that affect the efficiency and safety of the transportation network. The need for these decisions is paced by traffic, events, incidents, and emergencies that—with a few exceptions—cannot be anticipated in terms of exact timing and location. To maximize the quality and timeliness of the operational decisions needed, TMCs need the best possible real-time (or near-real time) situational information, communications, and detailed knowledge of the transportation network configuration. Most TMCs have significant investments in gathering and synthesizing situational information on the operational and physical aspects of the transportation network.

In many ways, EOCs and FCs have even greater decision-making challenges to address, because the right decisions have to be made quickly before, during, and after major incidents and emergencies occur—with significant potential impacts on public safety; multiple infrastructures; the economy; and often, national security. Although the centers may have some early warning on the risks of specific major incidents, events, and emergencies, the extent, location, and specific impacts on the public and infrastructure can usually not be fully assessed until the event, incident, or emergency is in process.

Although TMC managers and State DOTs understand that transportation network information is only a part of the information that EOCs and FCs synthesize, most believe that they monitor the best-available up-to-the minute situational awareness information regarding operations on the network. It is also apparent that the broader decisions and situational assessments made by EOCs and FCs have value to TMC operations before, during, and after incidents and emergencies affecting the TMC jurisdictions.

Chapter 3 of this guidebook identifies several potential kinds of data exchanges and communications that may be of value to at least two of the three center types, with discussions of the potential uses of these exchanges. *The focus of this guidebook (and Chapter 3) is on transportation-related information that is used, or may be used, in achieving the missions of some or many TMCs, EOCs, and FCs.* Practitioners of all three center types may review these exchange opportunities and assess the value gained through addressing and overcoming the issues and constraints involved in establishing means to implement some or many of the exchanges outlined.

What kinds of values/benefits should be considered? Some suggested considerations include:

- Savings in the costs of rapidly assembling situational information and keeping it current when needed, versus savings in leveraging current network data maintained by TMCs. Quickly obtaining situational knowledge is an expensive and unreliable process if

the means have not been developed to quickly tap, share, and corroborate existing information.

- The value of diverting staff from collecting and "scrubbing" data to the real functions of the center—assessing situations and making sound operational and risk judgments.
- Reduced "decision-risk" through supplemented or corroborative situational information. The potential costs of poor or untimely emergency or threat management decisions based on limited or unreliable facts could be very high in terms of hazards to the public, security, or economic and political fallout.
- The value of better common information held and utilized by TMCs, EOCs, and FCs. A greater number of agencies involved in a major incident raises the likelihood that not all agencies are acting on the same basic information, increasing the opportunity for conflicting or less-than-ideal incident management. Normal communication facilities may be down or disrupted, and redundant information channels may be needed.
- The value of routine, pre-arranged information exchange before and during an incident. Telephone and Internet access could be disrupted, and normal points of contact for information may not be reached or established at the right times. Messages may not be received and relayed properly, or agencies needing information may not get it through ad hoc channels.
- The value of improved utilization of ITS assets and other data-gathering assets already deployed in the region.
- Potential savings on deployment of new ITS and other data-gathering assets for common use.
- The value of improved inter-center communications and better interpretation of available data through common use and experience with the formats and protocols used by the "source" agencies.

What are the key issues and questions that should be explored by centers in evaluating information exchange opportunities? An initial checklist includes:

- What is available in this data that we do not already have?
- If it is nearly the same, can we save by sharing the cost of information acquisition once, rather than twice?
- Are there opportunities for sharing?
- Will information granularity or detail be improved by this exchange?
- What investment in time or equipment do we need to take advantage of the information?
- Can our policies on IT systems, data privacy, security, and firewalls accommodate this exchange, or can reasonable adjustments be made for compatibility?

- Do we need to adjust or manipulate the information to fit with our formats, conventions, or protocols for it to useful (e.g., location referencing)?
- Do we have sufficient communications and data management resources to make it work?
- Can we work around hours/days-of operation differences to communicate the information when needed?
- Are there other opportunities for cost savings to offset potential costs?
- Can we envision a case where better information, better corroboration, or more timely data would have improved our service or products? How do we value this?

The center-to-center dialogue on information, beginning with suggested opportunities in Chapter 3 and the initial checklist questions above, can lead to an objective assessment of information-specific and center-specific information exchange opportunities. The intent is for each center to consider the issues in terms of its own mission, jurisdiction, management challenges, and existing operating environment.

APPENDIX A. REFERENCES

511 Deployment Coalition, *Deployment Assistance Report #2, Transfer of 511 Calls to 911*, March 2002.

Agua Caliente, Band of Cahuilla Indians, "ACBCI Staff Visit the Palm Springs Emergency Operations Center," November 16, 2009, http://www.aguacaliente.org/GovernmentAffairsPress/tabid/55/Default.aspx#emergencyoperations, accessed 2010.

American Civil Liberties Union, "What's Wrong with Fusion Centers," December 5 2007, http://www.aclu.org/technology-and-liberty/whats-wrong-fusion-centers-executive-summary, accessed 2010.

Christin, Paul, and Stampfli, David, *Establishing Data Fusion Center Baseline Technology Capabilities*, 2009, http://proceedings.esri.com/library/userconf/hss09/homeland/papers/establishing_data_fusion_center_baseline_technology_capabilities.pdf, accessed 2010.

Congressional Research Service Report for Congress, John Rollins, *Fusion Centers: Issues and Options for Congress*, January 18, 2008, http://opencrs.com/document/RL34070, accessed 2010.

Consensus Systems Technologies, *New Mexico Statewide ITS Architecture Sausage Diagram*, http://www.consystec.com/nm/web/files/rptpdfs/rptSausageDiagram.pdf, accessed 2010.

Dallas County Office of Security and Emergency Management, "Emergency Operations Center Status," http://www.dallascounty.org/department/osem/status.html, accessed 2010.

Federal Emergency Management Agency and Emergency Management Institute, National Incident Management System, 2008.

Government Accountability Office, *Homeland Security: Federal Efforts are Helping to Address Some Challenges Faced by State and Local Fusion Centers*, April 2007.

Government Accountability Office, *Report to Congressional Committees: Homeland Security, Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State and Local Information Fusion Centers*, October 2007.

Government Accountability Office, *Testimony Before the Ad Hoc Subcommittee on State, Local, and Private Sector Preparedness and Integration, Committee on Homeland Security and Government Affairs, U.S. Senate*, April 17, 2008.

Harris, Blake, "Fusion Centers May Strengthen Emergency Management," *Government Technology*, May 30, 2008, http://www.govtech.com/em/365393, accessed 2010.

Institute for Intergovernmental Research Web site. Regional Information Sharing Systems (RISS). http://www.iir.com, accessed 2010.

Institute of Transportation Studies at the University of California at Berkeley and Caltrans, Sreedevi, Indu, *Services and Technologies: Transportation Management Centers*, http://www.calccit.org/itsdecision/serv_and_tech/Traffic_management/TMC/tmc_summary.html, accessed 2010.

International Association of Fire Chiefs, National Hazardous Materials Fusion Center, http://www.iafc.org/displayindustryarticle.cfm?articlenbr=36127, accessed 2010.

Kaplan, Eben, *Fusion Centers*, Council on Foreign Relations, February 22, 2007, http://www.cfr.org/publication/12689/, accessed 2010.

Kimley-Horn & Associates, *Bay Area Freeway Concept of Operations: Key Institutional and Technical Issues*, September 2001.

National Cooperative Highway Research Program (NCHRP), *Report 520: Sharing Information between Public Safety and Transportation Agencies for Traffic Incident Management*, 2004.

New York State Department of Transportation Traffic Engineering and Highway Safety Division, *Policy for Design and Operation of Closed-Circuit Television (CCTV) in Advanced Traffic Management Systems*, September 4, 2001, https://www.nysdot.gov/divisions/operating/oom/transportation-systems/systems-optimization-section/ny-moves/repository/mov_tv_policy.pdf, accessed 2010.

Oklahoma Office of Homeland Security, *DHS Announces $34 Million in FY 2009 Emergency Operations Center Grants*, December 16, 2008, http://www.ok.gov/homeland/News/2008/December_2008/DHS_ANNOUNCES_$34_MILLION_IN_FY_2009_EMERGENCY_OPERATIONS_CENTER_GRANTS.html, accessed 2010.

Price, R.G., "Territories, Possessions, and Influenced Areas of the United States of America," http://rationalrevolution.net/articles/territories.htm, accessed 2010.

Texas Department of Transportation, Texas Transportation Institute and The Texas A&M University System, *Houston TranStar Annual Report 2003*, http://www.houstontranstar.org/about_transtar/docs/Annual_2003_TranStar.pdf, accessed 2010.

Traffic Management Centers (TMCs) and ITS, http://tmcinfo.blogspot.com, accessed 2010.

U.S. Congress, *Implementing Recommendations of the 9/11 Commission Act of 2007*, http://www.govtrack.us/congress/billtext.xpd?bill=h110-1, accessed 2010.

U.S. Department of Homeland Security, *Fact Sheet: Homeland Security Information Network*, May 28, 2004, http://www.dhs.gov/xnews/releases/press_release_0418.shtm, accessed 2010.

U.S. Department of Homeland Security, *Information Sharing Strategy*, April 2008.

U.S. Department of Homeland Security, National Incident Management System, March 1, 2004, p. 129.

U.S. Department of Homeland Security, National Response Framework, January 2008.

U.S. Department of Homeland Security and U.S. Department of Justice, *Baseline Capabilities for State and Major Urban Area Fusion Centers – A Supplement to the Fusion Center Guidelines*, September 2008. http://it.ojp.gov/documents/baselinecapabilitiesa.pdf, accessed 2010.

U.S. Department of Justice, 28 CFR Part 23, *Criminal Intelligence Systems Operating Policies*, 1998.

U.S. Department of Justice, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*, January 2008.

U.S. Department of Transportation, Booz Allen Hamilton Inc. and Kimley-Horn and Associates, Inc., *Transportation Management Center Business Planning and Plans Handbook*, December 2005, http://tmcpfs.ops.fhwa.dot.gov/cfprojects/uploaded_files/TMC_BPG_Final.pdf, accessed 2010.

U.S. Department of Transportation, *Computer-Aided Dispatch - Traffic Management Center Field Operational Test: State of Utah Final Report, ITS Program Assessment Support Contract*, July 2006.

U.S. Department of Transportation, *Computer-Aided Dispatch - Traffic Management Center Field Operational Test: Washington State Final Report*, May 2006.

U.S. Department of Transportation, *Getting More by Working Together: Opportunities for Linking Planning and Operations*, November 2004, http://ops.fhwa.dot.gov/publications/lpo_ref_guide/index.htm, accessed 2010.

U.S. Department of Transportation, Haas, Robert, et al., i*Florida Model Deployment Final Evaluation Report*, January 2009, http://ops.fhwa.dot.gov/publications/fhwahop08050/index.htm, accessed 2010.

U.S. Department of Transportation, *ITS Deployment Statistics*, 2004.

U.S. Department of Transportation, *Metropolitan Transportation Management Center, A Case Study: Boston Central Artery/Tunnel Integrated Project Control System*, October 1999, http://ntl.bts.gov/lib/jpodocs/repts_te/11063.pdf, accessed 2010.

U.S. Department of Transportation, *Metropolitan Transportation Management Center, A Cross-Cutting Study: Improving Transportation, Network Efficiency*, October 1999, http://www.itsdocs.fhwa.dot.gov/JPODOCS/REPTS_TE/10923.pdf, accessed 2010.

U.S. Department of Transportation, *Recovery and Mitigation for Transportation Management Centers*, February 2007.

U.S. Department of Transportation, Research and Innovative Technology Administration (RITA), Intelligent Transportation System: Deployment Statistics, http://www.itsdeployment.its.dot.gov, accessed 2010.

U.S. Department of Transportation, Seymour, Edward J., *Handbook for Developing a TMC Operations Manual*, November 2005.

U.S. Department of Transportation, *Simplified Guide to the Incident Command System for Transportation Professionals*, February 2006, http://ops.fhwa.dot.gov/publications/ics_guide/index.htm, accessed 2010.

U.S. Department of Transportation, Smith, Brian, *Configuration Management for Transportation Management Systems*, September 2003, http://ops.fhwa.dot.gov/freewaymgmt/publications/cm/handbook/cmtmshb.pdf, accessed 2010.

Jeff Sangillo

National Security Agency Operations Center

APPENDIX B. TMC AND FC LOCATIONS

The following summarizes existing TMCs and the FCs across the United States that were identified as part of the research for this guidebook. It is not an exhaustive list, as additional facilities may exist in other locations or have opened since the initial research was completed. The list of FCs and RICs in Table B-1 was compiled from a variety of sources, as there is no public listing of all such centers in the United States. The centers listed here are all that could be readily identified as part of the research.

- Albany, Schenectady, Troy, NY
- Albuquerque, NM
- Allentown, Bethlehem, Easton, PA
- Asheville, NC
- Atlanta, GA
- Austin, TX
- Bakersfield, CA
- Baltimore, MD
- Baton Rouge, LA
- Beaumont-Port Arthur, TX
- Bellingham, WA
- Birmingham, AL
- Boise City, ID
- Boston, Lawrence, Salem, MA
- Buffalo, Niagara Falls, NY
- Charleston, SC
- Charlotte, Gastonia, Rock Hill, NC
- Chattanooga, TN
- Chicago, Gary, Lake County, IL
- Cincinnati, Hamilton, OH
- Cleveland, Akron, Lorain, OH
- Columbia, SC
- Columbus, OH
- Dallas, Fort Worth, TX
- Dayton, Springfield, OH
- Daytona Beach, FL
- Denver, Boulder, CO
- Des Moines, IA
- Detroit, Ann Arbor, MI
- El Paso, TX
- Eugene, OR
- Fort Myers, FL

- Fort Wayne, IN
- Fresno, CA
- Grand Rapids, MI
- Greensboro, Winston-Salem, High Point, NC
- Greenville - Spartanburg, SC
- Hampton Roads, VA
- Harrisburg, Lebanon, Carlisle, PA
- Hartford, New Britain, Middletown, CT
- Honolulu, HI
- Houston, Galveston, Brazoria, TX
- Huntsville, AL
- Indianapolis, IN
- Jackson, MS
- Jacksonville, FL
- Janesville-Beloit, WI
- Kansas City, KS
- Knoxville, TN
- Las Vegas, NV
- Little Rock, North Little Rock, AK
- Los Angeles, Anaheim, Riverside, CA
- Louisville, KY
- McAllen, TX
- Memphis, TN
- Miami, Fort Lauderdale, FL
- Milwaukee, Racine, WI
- Minneapolis, St. Paul, MN
- Modesto, CA
- Montgomery, AL
- Nashville, TN
- New Haven, Meriden, CT
- New London, CT
- New Orleans, LA
- New York, Northern New Jersey, Southwestern Connecticut
- Oklahoma City, OK
- Omaha, NE
- Orlando, FL
- Pensacola, FL
- Philadelphia, Wilmington, Trenton, PA
- Phoenix, AZ
- Pittsburgh, Beaver Valley, PA
- Portland, Vancouver, WA
- Providence, Pawtucket (RI), Fall River. (MA)

- Provo – Orem, UT
- Raleigh-Durham, NC
- Reno, NV
- Richmond, Petersburg, VA
- Roanoke, VA
- Rochester, MN
- Sacramento, CA
- Salinas, CA
- Salt Lake City, Ogden, UT
- San Antonio, TX
- San Diego, CA
- San Francisco, Oakland, San Jose, CA
- San Luis Obispo, CA
- Santa Barbara, CA
- Sarasota-Bradenton, FL
- Scranton, Wilkes-Barre, PA
- Seattle, Tacoma, WA
- Spokane, WA
- Springfield, MA
- Springfield, MO
- St. Louis, MO
- Stockton, CA
- Syracuse, NY
- Tampa, St. Petersburg, Clearwater, FL
- Toledo, OH
- Tucson, AZ
- Tulsa, OK
- Washington, DC
- West Palm Beach, Boca Raton, Delray, FL
- Wichita, KS
- Youngstown, Warren, OH

Table B-1: FC and RIC Locations and Functions Supported

State	Name of Fusion Center	All Crimes	All Hazards	Counterterrorism
Alabama	Alabama Information Fusion Center	x		
Alaska	Alaska Fusion Center	x	x	x
Arizona	Arizona Counter Terrorism Information Center (AcTIC)	x		
Arkansas	Arkansas Fusion Center	x	x	x

State	Name of Fusion Center	All Crimes	All Hazards	Counterterrorism
California	State Terrorism Threat Assessment Center (STTAC)	x		x
California	Los Angeles, Joint Regional Intelligence Center (JRIC)	x		x
California	Sacramento, Regional Terrorism Threat Assessment Center (RTTAC)	x		x
Colorado	Colorado Information Analysis Center (CIAC)	x	x	
Connecticut	Connecticut Intelligence Center (CTIC)	x		
Delaware	Delaware Information Analysis Center (DIAC)	x	x	
Florida	Florida Fusion Center	x	x	
Georgia	Georgia Information Sharing and Analysis Center (GISAC)		x	x
Hawaii	Hawaii Fusion Center		x	
Illinois	Chicago Crime Prevention and Information Center (CPIC)	x		x
Illinois	Statewide Terrorism and Intelligence Center (STIC)	x		
Indiana	Indiana Intelligence Fusion Center (IIFC)	x		
Iowa	Iowa Intelligence Fusion Center	x		
Kansas	Kansas Threat Integration Center (KSTIC)			x
Kentucky	Kentucky Intelligence Fusion Center (KIFC)	x		
Louisiana	Louisiana State Analysis and Fusion Exchange (La-SAFE)	x	x	
Maine	Maine Intelligence and Analysis Center			x
Maryland	Maryland Coordination and Analysis Center (MCAC)	x		x
Massachusetts	Commonwealth Fusion Center (CFC)	x		x

State	Name of Fusion Center	All Crimes	All Hazards	Counterterrorism
Michigan	Michigan Intelligence and Operations Center (MIOC)	x		
Michigan	Detroit and Southeastern Michigan Regional Fusion Center	x	x	x
Minnesota	Minnesota Joint Analysis Center (MN-JAC)	x	x	
Mississippi	Mississippi Analysis & Information Center	x	x	x
Missouri	Missouri Information Analysis Center	x	x	
Montana	Montana All-Threat Intelligence Center (MATIC)	x		
Nebraska	Nebraska Fusion Center	x	x	x
Nevada	Nevada Analytical and Information Center	x	x	x
New Hampshire	New Hampshire Fusion Center	x	x	
New Jersey	Regional Operations Intelligence Center (ROIC)	x	x	
New Mexico	New Mexico All Source Intelligence Center (NMASIC)	x	x	x
New York	New York Police Department (NYPD) Intelligence Division	x		x
New York	Rockland County Intelligence Center	x		
New York	New York State Intelligence Center (NYSIC)	x		
North Carolina	North Carolina Information Sharing and Analysis Center (ISAAC)	x		x
North Dakota	North Dakota Fusion Center	x	x	x
Ohio	Strategic Analysis and Information Center (SAIC)	x		x
Oklahoma	Oklahoma Information Fusion Center	x	x	

State	Name of Fusion Center	All Crimes	All Hazards	Counterterrorism
Oregon	Terrorism Intelligence and Threat Assessment Network (TITAN) Fusion Center	x	x	x
Pennsylvania	Pennsylvania Criminal Intelligence Center	x		
Rhode Island	Rhode Island Fusion Center			x
South Carolina	South Carolina Information Exchange (SCIEx)	x	x	
South Dakota	South Dakota Fusion Center	x	x	
Tennessee	Tennessee Regional Information Center (TRIC)	x		
Texas	North Central Texas Fusion Center (NTFC)	x	x	
Texas	Texas Fusion Center	x	x	
Utah	Utah Fusion Center	x	x	
Vermont	Vermont Fusion Center	x		
Virginia	Virginia Fusion Center		x	x
Washington	Washington Joint Analytical Center (WAJAC)	x	x	x
Washington, D.C.	Metropolitan Washington Fusion Center (MWFC)	x	x	
West Virginia	West Virginia Fusion Center	x	x	x
Wisconsin	Southeastern Wisconsin Terrorism Alert Center (STAC)	x	x	x
Wisconsin	Wisconsin Statewide Intelligence Center (WSIC)	x	x	x
Wyoming	Wyoming Office of Homeland Security			x

APPENDIX C. FC KEY DATA SOURCES

The research for this guidebook included a review of a number of sources, and this information is a compilation of that research. Databases that various FCs access include:

- State motor vehicle administrations – operators driver's license, vehicle registration, vehicle license tag information
- Location information (411, addresses, and phone numbers)
- Public records information (Accurint®)
- Law enforcement arrest and incarceration databases
- International Justice and Public Safety Information Sharing Network, and the Terrorist Screening Center (TSC)
- Public and private sources (security industry databases, identity theft databases, gaming industry databases)
- Regional Information Sharing Systems (RISS)/Law Enforcement Online (LEO)
- United States Private-Public Partnership (U.S.P3)—formerly HSIN-CI
- Organizational and association resources (InfraGard, The Infrastructure Security Partnership)
- Corrections (Bureau of Prisons, National Inmate Status)
- Sex offender registries
- Violent Criminal Apprehension Program (VICAP)
- Health- and public health-related databases (Public Health Information Network, Health Alert Network)
- Weapon permit information
- Internet Registry (American Registry for Internet Numbers – American Registry for Internet Numbers [ARIN]; Internet Service Provider [ISP] Information)
- CyberCop
- Federal Protective Service (FPS) Portal
- Lesson Learned Information Sharing (LLIS)
- National Counterterrorism Center (NCTC)
- Open Source Center

- Pentagon Force Protection Agency (PFPA)
- Regional Computer Forensics Group
- Federal Air Marshal Service (FAMS) Portal
- TRIPwire ATF information portal
- U.S. Secret Service e-Information Network
- U.S. Coast Guard Homeport information portal
- Real estate/tax information
- El Paso Intelligence Center (EPIC)
- FBI's National Date Exchange (N-DEx)
- FBI's Regional Data Exchange (R-DEx)
- Financial Crimes Enforcement Network (FinCEN)
- High Intensity Drug Trafficking Areas (HIDTA)
- Homeland Security Information Network (HSIN)
- International Association of Crime Analysts (IACA)
- International Association of Law Enforcement Intelligence Analysts (IALEIA)
- International Criminal Police Organization (INTERPOL)
- Law Enforcement Intelligence Unit (LEIU)
- National Crime Information Center (NCIC)
- National Drug Intelligence Center (NDIC)
- National White Collar Crime Center (NW3C)
- Nlets—The International Justice and Public Safety Information Sharing Network
- RISS Automated Trusted Information Exchange (ATIX)
- RISSNET™—RISSNET provides the six RISS centers with a secure criminal intelligence network for communications and information sharing by local, State, tribal, and Federal law enforcement agencies.
- Department of Defense (DoD) Internet Protocol Router Network (SIPRNet) – A secure network used to send classified data to select FC personnel with a Federal security clearance who will be able to access specific terrorism related information resident on the SIPRNet.[68]

68 DHS Announces New Information Sharing Tool to Help FCs Combat Terrorism, September 14, 2009. http://www.dhs.gov/ynews/releases/pr_1252955298184.shtm.

APPENDIX D. FUNDING AND RESPONSIBILITY CHART OF U.S. DOT, U.S. DOJ, DHS/FEMA

Table D-1: Primary Federal Funding Sources for TMCs, EOCs, and FCs

Funding Resource	Grant Type*	Eligible Activities	Eligible Recipients**		
			TMC	EOC	FC
FHWA					
National Highway System and Surface Transportation Program[i]	Formula	Transportation Operating, Capital	✓		
Congestion Mitigation and Air Quality Improvement Program (CMAQ)[ii]	Formula	Transportation Operating, Capital	✓		
National Highway Institute Training[iii]	Formula	Transportation Training	✓		
DHS Homeland Security Grant Program and FEMA Grants and Assistance Programs					
Emergency Operations Center (EOC) Grant Program [iv]	Discretionary	EOC Construction		✓	
Interoperable Emergency Communications Grant Program (IECGP)[v]	Discretionary	Planning, Training, Exercises for Communications	✓	✓	✓
Buffer Zone Protection Program[vi]	Discretionary	Prevention and Critical Infrastructure and Key Resource Capabilities		✓	✓
Competitive Training Grant Program (CTGP)[vii]	Discretionary	Training	✓	✓	✓
Emergency Management Performance Grants (EMPG)[viii]	Discretionary	Management Enhancements		✓	
Interoperable Emergency Communications Grant Program (IECGP)[ix]	Discretionary	Communications Equipment	✓	✓	✓

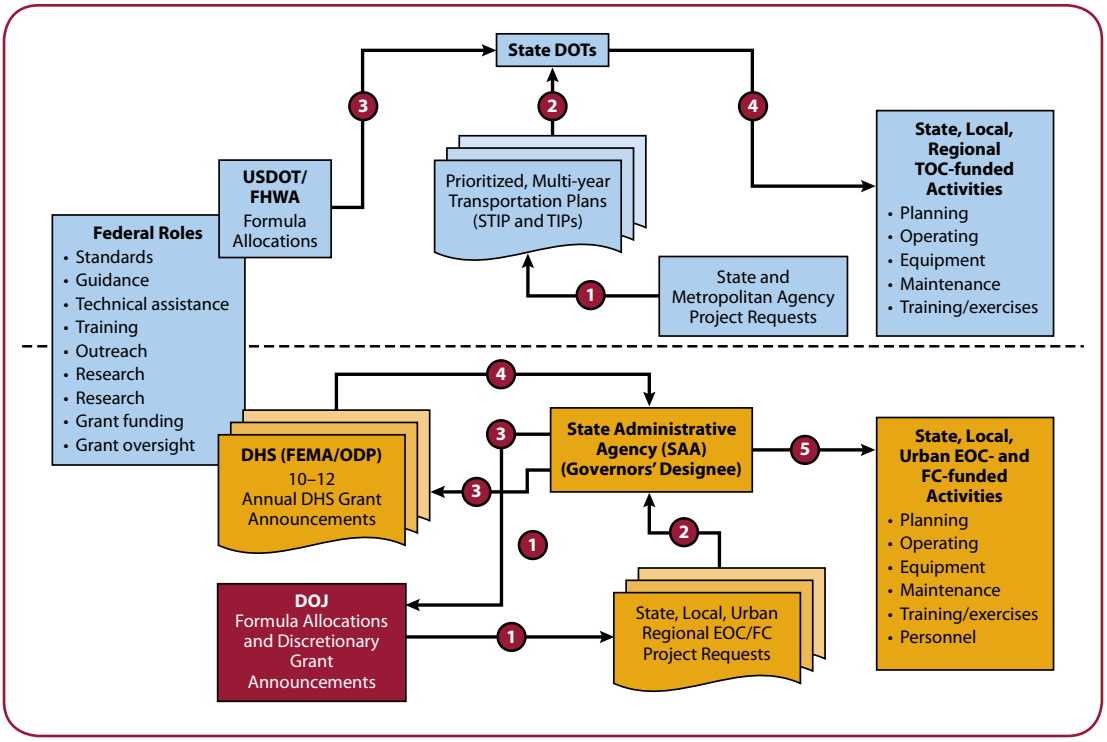
Funding Resource	Grant Type*	Eligible Activities	Eligible Recipients**		
			TMC	EOC	FC
State Homeland Security Program (SHSP)[x]	Discretionary	Planning, Organization, Equipment, Training, Exercises	✓	✓	✓
Urban Areas Security Initiative (UASI)[xi]	Discretionary among high-risk areas	Multidisciplinary Planning, Organization, Equipment, Training, Exercises	✓	✓	✓
Metropolitan Medical Response Program (MMRP)[xii]	Discretionary	Medical Response	✓	✓	✓
Operation Stonegarden (OPSG)[xiii]	Discretionary among land border states	Border Operations	✓	✓	✓
Regional Catastrophic Preparedness Grant Program (RCPGP)[xiv]	Discretionary	Integration Planning	✓	✓	✓
U.S. DOJ					
Justice Assistance Grant Program[xv]	Formula Block Grants	Crime Prevention Activities			✓
Antiterrorism and Emergency Assistance Program[xvi]	Discretionary	Victim Assistance		✓	✓
Bureau of Justice Assistance Discretionary grant programs[xvii]	Discretionary	Special Project			✓

***** *Decisions for FHWA funds are allocated by formula, and decisions for individual projects are made at the State or metropolitan planning organization level and are included in the State Transportation Improvement Plan (STIP) or metropolitan Transportation Improvement Plan (TIP). Most DHS and U.S. DOJ funds are allocated at the State level through the State Administrative Agency (the Governors' designee).*

*** While eligible recipients for some grant programs include all State and local agencies, often DOJ and DHS grant funds FC activities, DHS grants fund EOC activities, and DOT grants fund TOC activities. Programs where State and local agencies are eligible grant recipients may be opportunities for TMCs, EOCs, and FCs to submit a combined request.*

**** Program descriptions, eligibility, and application procedures for all Federal grant programs may be found in the Catalogue of Federal Domestic Assistance (https://cfda.gov). In addition, web pages for these specific programs are included in the footnote for each grant program below.*

Figure D-1: U.S. DOT, DHS, and U.S. DOJ Funding Diagram



[i] **FHWA National Highway System and Surface Transportation Program:** The operating costs for traffic monitoring, management, and control systems, such as integrated traffic control systems, incident management programs, and traffic control centers, are eligible for Federal reimbursement from National Highway System and Surface Transportation Program funding. Operating costs include labor costs, administrative costs, costs of utilities and rent, and other costs, including system maintenance costs, associated with the continuous operation of the system. For both National Highway System (NHS) and Surface Transportation Program (STP), the Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (SAFETEA-LU) continues the eligibility of capital and operating costs for traffic monitoring, management, and control facilities and programs. Also, the Transportation Equity Act for the 21st Century (TEA-21) clarified and SAFETEA-LU continues the eligibility of NHS and STP funds for ITS capital improvements to specifically allow funds to be spent for infrastructure-based ITS capital improvements.
http://www.fhwa.dot.gov/federalaid/projects.cfm

[ii] **FHWA Congestion Mitigation and Air Quality Improvement Program (CMAQ):** For projects located in air quality non-attainment and maintenance areas, and in accordance with the eligibility requirements of 23 USC 149(b), Congestion Mitigation and Air Quality Improvement Program funds may be used for operating costs for a 3-year period, so long as those systems measurably demonstrate reductions in traffic delays. Operating costs include labor costs, administrative costs, costs of utilities and rent, and other costs, including system maintenance costs, associated with the continuous operation of the system.
http://www.fhwa.dot.gov/environment/cmaqpgs/index.htm

[iii] **FHWA National Highway Institute:** States may use funds not to exceed one half of 1 percent of the amount apportioned to each State under Section 104(b)(3) for the surface transportation program for training their employees or employees of local transportation agencies. Such expenditures may not exceed 80 percent of the total cost of tuition and direct education expenses (excluding salaries) in connection with the education and training activities. Courses and study programs may be obtained from universities, other government agencies, the private sector, and/or the National Highway Institute. http://www.nhi.fhwa.dot.gov/home.aspx

[iv] **DHS Emergency Operations Center (EOC) Grant Program:** Intended to improve emergency management and preparedness capabilities by supporting flexible, sustainable, secure, and interoperable EOCs with a focus on addressing identified deficiencies and needs. Funds are available for grants for construction or renovation of a State, local, or tribal government's principal EOC. The State Administrative Agency (SAA) is the only eligible entity able to apply for the available funding on behalf of qualified State, local, and tribal EOCs.
http://www.fema.gov/government/grant/eoc/index.shtm

[v] **DHS Interoperable Emergency Communications Grant Program (IECGP):** Intended to improve local, tribal, regional, statewide, and national interoperable emergency communications, including communications in collective response to natural disasters, acts of terrorism, and other man-made disasters. Funds are available for planning, training, exercise, and personnel activities consistent with the goals and objectives of the Statewide Communication Interoperability Plans (SCIP) and aligned with the National Emergency Communications Plan (NECP). The State Administrative Agency is the only agency eligible to apply for FY 2008 IECGP funds. http://www.fema.gov/government/grant/iecgp/index.shtm

[vi] **DHS Buffer Zone Protection Program (BZPP):** BZPP provides grants to build security and risk-management capabilities at the State and local level to secure pre-designated Tier I and Tier II critical infrastructure sites, including chemical facilities, financial institutions, nuclear and electric power plants, dams, stadiums, and other high-risk/high-consequence facilities. Specific BZPP sites within 45 States have been selected based on their level of risk and criticality.
http://www.fema.gov/government/grant/bzpp/index.shtm

"DHS encourages projects funded through the FY 2010 BZPP to support the coordination and direct interaction with State, regional, and/or urban area fusion centers, and/or EOCs located in the region of the identified BZPP site. Examples include allowing fusion centers and/or EOCs access to video camera surveillance feeds resulting from cameras purchased through the BZPP or ensuring the jurisdiction responsible for the BZPP site has an identified liaison officer responsible for coordinating with and reporting suspicious activity to the fusion center." http://www.fema.gov/pdf/government/grant/2010/fy10_bzpp_kit.pdf. March 18, 2010

[vii] **DHS Competitive Training Grants Program (CTGP):** Awards funds to competitively selected applicants to develop and deliver innovative training programs addressing high-

priority national homeland security training needs.
http://www.fema.gov/emergency/ctgp/index.shtm

[viii] **DHS Emergency Management Performance Grants (EMPG):** Provides funds to assist State and local governments to sustain and enhance all-hazards emergency management capabilities.
http://www.fema.gov/government/grant/empg/index.shtm

[ix] **Interoperable Emergency Communications Grant Program (IECGP):** Provides funds to improve local, tribal, regional, statewide, and national interoperable emergency communications, including ensuring communications in collective response to natural disasters, acts of terrorism, and other man-made disasters is available for planning, training, exercise, and personnel activities consistent with the goals and objectives of the SCIP and aligned with the NECP. http://www.fema.gov/government/grant/iecgp/index.shtm

[x] **DHS State Homeland Security Grant Program (SHSP):** Provides funds to build capabilities at the State and local levels through planning, organization, equipment, training, and exercise activities. SHSP also supports the implementation of State homeland security strategies and key elements of the national preparedness architecture, including the National Preparedness Guidelines, the NIMS, and the NRF. Eligible entities for SHSP are all 50 States, the District of Columbia, Puerto Rico, American Samoa, Guam, Northern Mariana Islands, and the Virgin Islands. Available funds are distributed to each State based upon the risk and effectiveness scores associated with each application and also on a minimum allocation consistent with the statutory formula set by the 9/11 Act.
http://www.fema.gov/government/grant/hsgp/index.shtm#1

[xi] **Urban Area Security Initiative (UASI):** Addresses the unique multi-disciplinary planning, organization, equipment, training, and exercise needs of high-threat, high-density urban areas, and assists them in building and sustaining capabilities to prevent, protect against, respond to, and recover from threats or acts of terrorism. This program provides funding to high-risk urban areas based on risk and effectiveness. Funds are allocated based on risk and anticipated effectiveness upon completion of the application review process. The 60 candidates are eligible to apply for funding under the UASI program.
http://www.fema.gov/government/grant/hsgp/index.shtm

[xii] **Metropolitan Medical Response System Program (MMRS)**: Grants support local preparedness efforts to respond to all-hazards mass casualty incidents, including epidemic disease outbreaks; natural disasters; large-scale hazardous materials incidents; and chemical, biological, radiological, nuclear or explosive attacks. Equal funding allocations are made to 124 cities to establish and sustain activities.
http://www.fema.gov/government/grant/hsgp/index.shtm#4

[xiii] **DHS Operation Stonegarden (OPSG):** Focuses on enhancing law enforcement preparedness and operational readiness along the land borders of the United States. OPSG provides funding to designated localities to enhance cooperation and coordination among Federal, State, tribal and local law enforcement agencies to secure the United States' land borders.
http://www.fema.gov/government/grant/opsg/index.shtm

[xiv] **DHS Regional Catastrophic Preparedness Grant Program (RCPGP):** Provides funding to advance catastrophic incident preparedness to pre-designated high-risk urban areas. The goal of RCPGP is to support an integrated planning system that enables regional all-hazard planning for catastrophic events and the development of necessary plans, protocols, and procedures to manage a catastrophic event.
http://www.fema.gov/government/grant/rcp/index.shtm

[xv] **U.S. DOJ Justice Assistance Grants (JAG):** Allows States and local governments to support a broad range of activities to prevent and control crime and to improve the criminal justice system. JAG replaces the Byrne Formula and Local Law Enforcement Block Grant (LLEBG) programs with a single funding mechanism that simplifies the administration process for grantees. Funds are allocated by a formula based on population and crime statistics, in combination with a minimum allocation to ensure that each State and territory receives an appropriate share. JAG funds can be used to pay for personnel, overtime, and equipment. Funds provided for the States can be used for statewide initiatives, technical assistance and training, and support for local and rural jurisdictions.
http://www.ojp.usdoj.gov/BJA/funding/current-opp.html

[xvi] **U.S. DOJ Antiterrorism and Emergency Assistance Program:** Provides assistance to jurisdictions to address victim needs in the aftermath of an act of terrorism or mass violence. Funds may be used to compensate and assist victims within or outside the United States.
http://www.ojp.usdoj.gov/ovc/fund/pdftxt/antiterrorapplication.pdf

[xvii] **Bureau of Justice Assistance Discretionary Programs (BJA):** Awards discretionary grants to local governments, States, American Indian and Alaska Native tribes and tribal organizations, educational institutions, private nonprofit organizations, and for-profit organizations. Some discretionary awards are competitive and make a pool of funds available to a targeted group of applicants. Examples of limited competition programs are the Drug Court Discretionary Grant Program, Gang Resistance Education and Training, Indian Alcohol and Substance Abuse Program, Justice and Mental Health Collaboration Program, Prescription Drug Monitoring Program, Prisoner Reentry Initiative, and Tribal Courts Assistance Program.
http://www.ojp.usdoj.gov/BJA/funding/current-opp.html

Appendix E. FC Interoperability Challenges

In 2008, in the results of the National Governors Association Center for Best Practices (NGA Center) annual survey of governors' homeland security advisors, survey respondents identified developing interoperable communications as the issue for which States most need Federal assistance—in the form of funding and guidance, with FCs serving as the primary method for sharing information with DHS.

In April 2008, the GAO revisited the areas of concern that it reported to the U.S. Senate Committee on Homeland Security and Government Affairs' Ad Hoc Subcommittee on State, Local, and Private Sector Preparedness and Integration. In the report, there were still areas where more work needed to be done, and the GAO reported that DHS and U.S. DOJ were still working to correct the problem areas.

Concerning interoperability, the GAO reports that DHS, U.S. DOJ, and the Program Manager for Information Sharing Environment (PM-ISE) have taken steps to give FCs more access to Federal information systems. Of the 43 FCs interviewed by the GAO, 40 reported having access to HSIN, 16 were awaiting access to the DHS classified network, 39 have access to LEO, and 23 are in the process of gaining access to FBI classified systems. However, while FCs are primarily designed to serve the jurisdictions within which they operate, thus purchasing systems that they feel best serve their needs, centers are working to overcome the issue of interoperability. FCs have developed a solution to interoperability by producing alerts, bulletins, reports, and assessment products that can be transmitted in an unclassified format over everyday mediums such as text, e-mail, and fax. This information is usually intended to educate and inform those individuals who have the right and need to know the information. However, phone calls are the most often-used method by FCs when dealing with outside agencies. Individuals identified in an agency as a person with "need to know" status or the appropriate clearance and "need to know" status can be the recipient of information from an FC despite a lack of formal interoperability between the FC and the other agency.

On the opposite end of a lack of interoperability and the lack of information is an FC receiving too much data. To tackle the concern over information overload in FCs, one strategy involves funneling information to the proper analysts.[69] For example, in the Virginia FC, information concerning a particular mode of transportation (e.g., rail, freight, and highway) would be reviewed by an expert specializing in that mode, while information about gangs would go to that analyst. "These folks are trained researchers," explains Richard W. Kelly, Director of New Jersey's FC. "They know what to look for when they stick a ladle into that great stream of information."[70] DHS, U.S. DOJ, and PM-ISE are also working to streamline

69 Kaplan, Eben, Fusion Centers, Council on Foreign Relations website. http://www.cfr.org/publication/12689/, February 22, 2007.

70 Ibid.

the information process. It has even been recommended to the GAO that DHS and U.S. DOJ limit the number of existing systems or develop a unified platform for information sharing between FCs and between FCs and the Federal government. Following the national FC conference held in March 2008, Charlie Allen, Under Secretary for Intelligence and Analysis at DHS, reported that DHS was committed to building a national FC network to connect the FCs in all 50 States and all major cities. Such a network would be the solution that could address many of the current FC issues. In 2009, Director Robert Riegle, State and Local Program Office, Office of Intelligence and Analysis, testified before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, that the use of a common FC backbone/platform for information sharing has been recognized as key to better information sharing and collaboration. FC directors indicated that leveraging the framework of the Suspicious Activity Reporting (SAR) Initiative could be beneficial in further standardizing the use of technology across the FC network.

Clearances and classification of documents is another concern. While DHS and US DOJ work to provide clearances to the backlog of individuals that need them, over-classification of documents can make information gathering or sharing slow for the FCs. Issues still are reported to exist between FBI and DHS accepting each other's clearances. This problem exists because each agency conducts its own clearance process resulting in gaps between the two organizations' processes. One solution to overcoming this issue is the deployment of DHS officials to 36 operational FCs across the country. In addition, the FBI has assigned 114 employees to assist in 38 FCs. These professional analysts will assist at the centers where they are assigned and could be used to help with the handling of classified materials above the level assigned to the analyst. Another strategy to overcome classification issues is to grant clearances at the top secret (TS) level. However, it is important to point out that an individual with a TS may not necessarily have "need to know" status either. For outside agencies working with FCs, having an individual in that agency with "need to know" status or having the appropriate clearance and "need to know" status will aid them in receiving the information needed from the FC to complete its mission.

The August 2006, FC Guidelines were designed to provide guidance, technical assistance, and training to FCs. Based on the April 2007 GAO report, this area still needs to be addressed further. Until FCs are able to receive the type of training and guidance they report to need, training of partner agencies will be difficult. The March 2008 national FC conference saw the establishment of baseline-level FC capabilities; however, feedback is pending. In the meantime, FCs like the Michigan Intelligence Operation Center have begun to offer various forms of training for local law enforcement and partners of the intelligence cycle. This solution by outreach not only trains partner agencies that may not be familiar with the needs of and products produced by the FCs but also builds stronger relationships and a better understanding for one another.

APPENDIX F. TOP SITES TO BENEFIT FROM COLLABORATION

FHWA has an interest in encouraging State and local TMCs, EOCs, and FCs to establish more effective communication links and promote information sharing. Some metropolitan areas already have at least one TMC, EOC, and FC in close proximity to each other, creating a situation where each of the three centers would likely have interest in similar information, the bulk of which was discussed in Chapter 3 of this guidebook.

Table F-1 provides a list of sites where collaboration between TMCs, EOCs, and FCs would most likely be successful. These sites were chosen based on the following criteria:

- Metropolitan area
- Established TMC, EOC, and FC in close proximity to each other
- Robust TMC that will be able to provide transportation-related information to the EOC and FC.

Some of the sites on this list already work closely with the other sites in their vicinity through partnerships and information-sharing agreements. In addition to outlining potential areas where greater connectivity could be achieved, the list also provides a resource for lesser-developed sites as to the potential sites on which new information-sharing programs might be based.

Table F-1: Top Sites to Benefit from TMC-EOC-FC Collaboration

TMC	EOC	FC	City	State
City of Phoenix Transportation Management Center	State EOC is located on the Papago Park Military Reservation	Arizona Counter Terrorism Information Center (ACTIC)	Phoenix	AZ
Los Angeles Regional Transportation Management Center	County of Los Angeles' Emergency Operations Center (EOC)	Regional Terrorism Threat Assessment Center (RTTAC)/Los Angeles/Joint Regional Intelligence Center	Los Angeles	CA
Caltrans District 3 Regional Transportation Management Center	Sacramento Regional Homeland Security and Emergency Management Training Center	State Terrorism Threat Assessment Center/ Sacramento Regional Terrorism Threat Assessment Center	Sacramento	CA

TMC	EOC	FC	City	State
Colorado Transportation Management System	Denver Emergency Operations Center	Colorado Information Analysis Center	Denver-area	CO
Deltrac Transportation Management Center	Delaware Emergency Management Operations Center	Delaware Information Analysis Center	Dover-area	DE
Georgia NaviGAtor	Atlanta-Fulton County Emergency Operations Center	Georgia Information Sharing and Analysis Center	Atlanta	GA
Gary-Chicago-Milwaukee (GCM) Corridor Transportation Information Center	City of Chicago Joint Operations Center	Chicago Crime Prevention and Information Center	Chicago	IL
Indianapolis TrafficWise	State of Indiana Emergency Operations Center	Indiana Intelligence Fusion Center	Indianapolis	IN
Kentucky Transportation Operations Center	State Emergency Operations Center	Kentucky Intelligence Fusion Center	Frankfort	KY
Advanced Traffic Management and Emergency Operations Center	Advanced Traffic Management and Emergency Operations Center	Louisiana State Analytical and Fusion Exchange (LA-SAFE)	Baton Rouge	LA
Boston Transportation Department Traffic Management Center	Boston Emergency Operations Center	Commonwealth Fusion Center/Boston Regional Intelligence Center	Boston	MA
Intelligent Transportation Systems Center	SE Michigan Detroit Edison Emergency Operations Center	Michigan Intelligence Operations Center	Detroit	MI
Regional Transportation Management Center	City of Minneapolis Emergency Operations Center	Minnesota Joint Analysis Center	Minneapolis-area	MN
Triangle Transportation Management Center	Wake County Emergency Operations Center	North Carolina Information Sharing and Analysis Center (ISAAC)	Raleigh	NC

TMC	EOC	FC	City	State
DalTrans Transportation Management Center	Dallas County Emergency Operations Center	North Central Texas Fusion Center	Dallas	TX
Greater Houston Transportation and Emergency Management Center	Greater Houston Transportation and Emergency Management Center	Houston Regional Intelligence Service Center	Houston	TX
WSDOT Traffic Systems Management Center (TSMC)	Fire Station 10 Emergency Operations Center	Washington State Joint Analytical Center	Seattle	WA
MONITOR Transportation Management Center	Milwaukee Emergency Operations Center	Southeast Wisconsin Terrorism Alert Center (STAC)	Milwaukee	WS

This page left intentionally blank.

APPENDIX G. TECHNICAL CONSIDERATIONS AND VULNERABILITY IMPROVEMENTS

Introduction

ITS are vulnerable to a variety of disruptions, both naturally occurring, such as hurricanes and earthquakes, and man-made, including power outages and hazardous materials. To ensure uninterrupted functionality of ITS technologies, it is necessary to plan for such disasters. Planning for supply and other varieties of disruptions involves the design and implementation of a backup system that duplicates some of the most important functions of the original system; planning for a large-scale community-wide incident; and the management, testing, and documentation for backup systems to ensure their functionality in case of primary system failures.

Backup System Strategies

If the primary TMC site becomes unavailable, an alternate site should be identified for a backup system, for which plans have been documented. Four alternate site possibilities exist. Each provides different features and relative costs. Ordered from most to least costly, they include redundant site, hot site, cold site, and cooperative agreement. Additionally, there are derivatives of each type.

A redundant site entails a second operations center that is always standing ready with the hardware, software, and communications infrastructure already in place and running. This backup site may take over operations at any point needed, without any specific startup to execute. With the availability of a redundant site, part of the operations may always be run from the second site. In this scenario, the only difference that would occur during a system outage at the primary site would be that all staff would work from the one operations center rather than being spread over two installations. While the fastest mode of recovery, it is normally the most expensive. Another issue with a redundant site is that it normally resides close to the main operations center. If the incident is community-wide, both the primary and redundant sites may become inoperable.

A hot site is an operations center that is set up with all the needed hardware and network infrastructure, but lacking the necessary software for normal operations. Hot sites are normally shared by several different organizations, serving as backup sites for agencies on a first-come first-serve basis. If a community-wide incident occurs, it is possible that the hot site may not be available. Such an incident may require transfer to an alternate site in a different region or the possibility of having no site available to meet agency needs. If open, the hot site is immediately available upon the declaration of an emergency. Before becoming operational, the site must be restored with the operating organization's software. Hot sites are normally subscription services where an annual fee is paid providing for testing

time and the ability to use a site if needed. Use of the site for an emergency is frequently at an additional cost.

Cold sites provide the infrastructure of a building as well as some wiring; heating, ventilation and air conditioning (HVAC); and a private branch exchange (PBX). If movement to a cold site is necessary, rooms may then be quickly filled by the occupying organization with hardware to run operations. Setting up operations in a cold site will take longer than either a redundant site or hot site, but use is generally less costly. Depending upon the exact requirements, a cold site may be able to be delivered to a desired location via a trailer, or may be a quickly constructed building. Frequently, a cold site is utilized after an initial period of time spent in a hot site.

The least costly alternative is a cooperative agreement, a reciprocal accord with either another municipal agency in the region or an equivalent agency in an adjoining municipality. These agreements frequently have little or no cost associated for rental of the space. While inexpensive, exercising cooperative agreements can be difficult in an emergency. Because many agency operations managers are asked to work with as few resources as possible while maintaining a high level of service to their customers, it is uncommon that operations centers would have enough extra equipment and space to enable an influx of all of the personnel and work from another operations center, which may last for a considerable amount of time. Also unlikely is the ability to periodically take space from an existing operation to test a contingency plan.

Regardless of the nature of the backup system, several issues need to be addressed:

- All software licenses must allow for running the system at an alternate location for either tests of emergency situations or true emergencies.
- Any backup files that exist must also be able to be easily and quickly transported or communicated to the alternate site.
- Communications lines that normally terminate in an operations center must be able to be rerouted to the alternate center.

Planning

While planning for a backup TMC system, the planner must expect and account for the unexpected. An example of an unexpected system failure was the Great Lakes Blackout in 2003. This blackout was initiated by a brush fire that knocked out a single power line south of Columbus, Ohio. This was followed by the failure of a second power line connecting eastern and northern Ohio, which in turn was followed by the failure of a third power line in northern Ohio due to excess loading. As more power lines progressively started to disconnect from the grid, the failures accelerated. Five power lines between Ohio and Michigan failed about 8 minutes after the first failure. This led to failure of the entire power system around the Great Lakes region, leaving cities from Cleveland to the cities in the East Coast like New York in a profound blackout. This incident was the initiator of a cascading set of failures, leading to a vast swath of 3,700 miles of North America without power. A set of

seemingly minor failures acting in concert led to the largest blackout in American history. These minor incidents acting in concert were not expected, eventually having a devastating impact. A compounding of minor incidents leading to major disaster is often true of many community-wide disasters.

During such periods of operational recovery and mitigation, most TMCs have found that significant problems exist with communications. To avoid such problems, state-of-the-art communications practice for TMCs includes the use of multiple communications paths, which ideally avoid systems outages. By maintaining multiple communications paths, the TMC is able to avoid a systems outage based on a single communications outage from a single central office or an individual line. It is also possible that during emergencies and outages, telephone calls from TMCs cannot be completed even if the system is available due to excessive phone calls from system users inquiring about the nature of the incident and the welfare of the area. TMCs could circumvent these problems by utilizing the Government Emergency Telecommunication System (GETS). Another provision that TMCs could use is voice telephones that do not require electricity for operations. Mitigation of power supply problems could be accomplished by having multiple feeds from various power stations or grids. Finally, in case of the entire grid or multiple power station failure, TMCs could utilize Uninterrupted Power Supply (UPS) systems to supply emergency power.

Good planning mitigates the effects of unexpected system failures. An example of good planning and interagency cooperation was demonstrated during the New York City Blackout of August 2003. The I-95 Corridor Coalition contacted member agencies that were not affected by the blackout to post messages informing motorists of the problem. The notification allowed the motorists the ability to avoid the affected areas, helping to relieve traffic congestion in the New York City area. Another method to ensure the functionality of the system during community-wide emergencies is that of working from alternative sites. These sites may include connecting into the system from the staff member's home or an alternate office arrangement. By connecting into the system from an alternative location, fundamental goals of the TMC may be handled without full access to the operations center.

Testing

Testing of a backup system provides a number of benefits to a TMC. One of the most important benefits that the test provides is an initial and continuous validation of the TMC backup plan. Another important benefit to testing is the evaluation of the effects that external interfaces and changes to the TMC have on the recovery and mitigation plan.

Documentation

Recovery and mitigation documents must be confidential yet widely available to TMC staff. The documentation must have all the information needed to rapidly reconstruct the TMC.

Network layouts, security infrastructure, systems complexities, internal procedures, and complete staff contact lists are some of the critical and confidential information that must be included in a plan. During system outages and emergency TMC relocation, the

documentation must be available away from the operations center. Some TMCs make the documentation available through the Internet. In these cases, the documentation must be stored in servers that are not co-located with the TMC. Others centers provide the document in full or in part in hardcopy or on various softcopy devices such as CDs or thumb drives.

APPENDIX H. INVENTORY OF TRAINING RESOURCES

Training resources include the following:

IS-700, NIMS: An Introduction
Emergency Management Institute, Independent Self-study Program
http://training.fema.gov/emiweb/is/is700.asp

IS-800, National Response Framework: An Introduction
Emergency Management Institute, Independent Self-study Program
http://training.fema.gov/emiweb/is/is800b.asp

ICS-100, Introduction to the Incident Command System
Emergency Management Institute, Independent Self-study Program
http://training.fema.gov/emiweb/is/is100.asp

ICS-200, ICS for Single Resources and Initial Action Incidents
Emergency Management Institute, Independent Self-study Program
http://training.fema.gov/emiweb/is/is200.asp

ICS-300, Intermediate ICS for Expanding Incidents
Emergency Management Institute Training Catalog, page 150. Available at:
http://training.fema.gov/EMICourses/EMICatalog.asp
Course is available through individual State training officers.

FHWA's Simplified Guide to the ICS for Transportation Professionals
Available at: http://ops.fhwa.dot.gov/publications/ics_guide/index.htm

Criminal Intelligence Systems Operating Policies (28 CFR, Part 23)
Training Institute for Governmental Research, Law Enforcement Research and Training
Information available at: http://www.iir.com/28cfr/

State and Local Anti-terrorism Training (SLATT)
Institute for Governmental Research, Law Enforcement Research and Training
Information available at: http://www.iir.com/slatt/

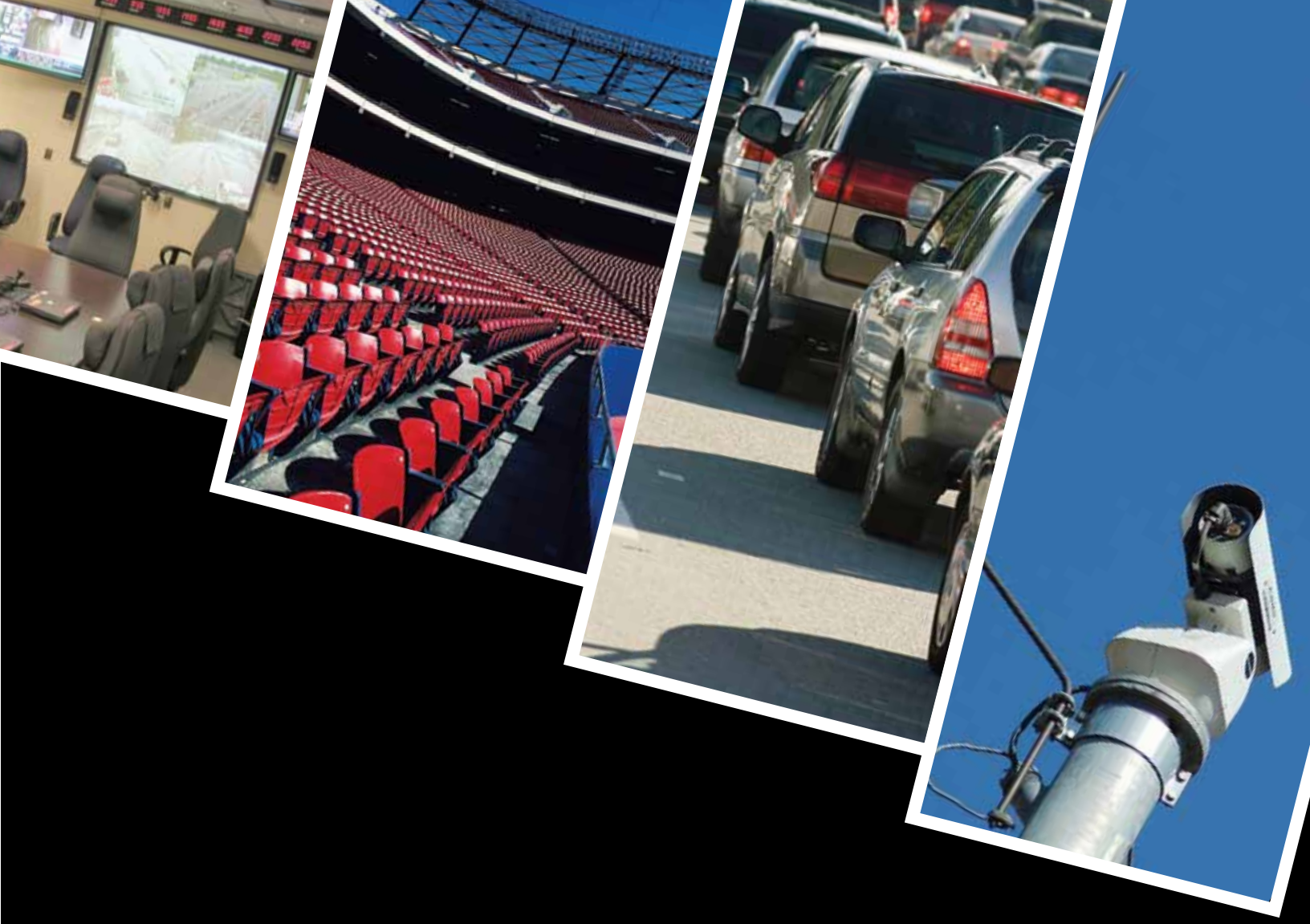
Anti-Terrorism Intelligence Awareness Training Program (AIATP)
Federal Law Enforcement Training Center
Information available at: http://www.fletc.gov/training/programs/state-local/training-opportunities/anti-terrorism-intelligence-awareness-training-program-aiatp/

Multi-discipline, multi-jurisdictional all-hazards exercises include the following:

IS-120, An Introduction to Exercises
Emergency Management Institute, Interactive Web-based course
http://training.fema.gov/EMIWeb/IS/IS120A.asp

IS-130, Exercise Evaluation and Improvement Planning
Emergency Management Institute, Interactive Web-based course
http://training.fema.gov/EMIWeb/IS/IS130.asp

Exercise participation
Information on scheduled Homeland Security Exercise and Evaluation Program (HSEEP) exercises may be found at: https://hseep.dhs.gov/pages/1001_HSEEP7.aspx



U.S. Department of Transportation
Federal Highway Administration
Office of Operations
1200 New Jersey Avenue, SE
Washington, DC 20590
www.ops.fhwa.dot.gov
FHWA-HOP-09-003
June 2010